IAIS

INTERNATIONAL ASSOCIATION OF
INSURANCE SUPERVISORS

INSURANCE CORE PRINCIPLES, STANDARDS, GUIDANCE AND ASSESSMENT METHODOLOGY

ICP 8

Revisions for consultation
June 2015

Version with track changes

ICP 8 Risk Management and Internal Controls

The supervisor requires an insurer to have, as part of its overall corporate governance framework, effective systems of risk management and internal controls, including effective functions for risk management, compliance, actuarial matters and internal audit.

Introductory Guidance

8.0.1 As part of the overall corporate governance framework and in furtherance of the safe and sound operation of the insurer and the protection of policyholders, the Board[1] is ultimately responsible for ensuring~~overseeing~~ that the insurer has in place effective systems of risk management and internal controls[2] and functions to address the key risks it faces and for the key legal and regulatory obligations that apply to it. ~~, and that~~ Senior Management effectively implements these systems ~~properly~~ and provides the necessary resources and support for these functions.

8.0.2 The systems and functions should be adequate for ~~the nature, scale, and complexity of~~ the insurer's objectives~~-~~, strategy, risk profile, and the applicable legal and regulatory requirements. ~~business and risks and~~ They should be adapted as the insurer's business and internal and external circumstances change.

8.0.3 The nature of the systems that the insurer has is dependent on many factors. ~~These include the insurer's risk profile and the applicable legal and regulatory requirements.~~ The~~se~~ systems typically include:

- strategies setting out the approach of the insurer for dealing with specific areas of risk and legal and regulatory obligation;
- policies defining the procedures and other requirements that members of the Board and employees need to follow

[1] Differences between one-tier and two-tier board systems of governance are dealt with in the introduction to ICP 7 Corporate Governance.

[2] While risk management and internal controls are discussed separately in this document, some supervisors or insurers may use "internal controls" as an umbrella term to include the functions of risk management, internal audit, compliance and, actuarial, while others may consider internal controls a subset of the risk management system. The two terms are in fact closely related. Consensus on where the boundary lies between risk management and internal controls is less important than achieving, in practice, the objectives of each.

~~and policies for identification, aggregation and mitigation of risks~~;

- processes for the implementation of the insurer's strategies and policies; and
- controls to ensure that such strategies, policies and processes are in fact in place, are being observed and are attaining their intended objectives.

~~8.0.4 The risk management system of an insurer comprises the totality of strategies, policies, processes and controls for identifying, assessing, monitoring, managing and reporting risks to which the insurer may be exposed at a legal entity and group-wide level.~~

~~8.0.5 The totality of all controls an insurer has in place is generally referred to as the internal controls system.~~

Comment [U11]: Deleted. Definition in Glossary

~~8.0.6~~8.0.4 An insurer's ~~also has properly authorised~~ functions (whether in the form of a person, unit or department) should be properly authorised to carry out specific activities relating to matters such as risk management, compliance, actuarial matters and internal audit. These are generally referred to as control functions~~. Subject to Guidance 8.2.8 and Standard 8.7 below, and to the nature, scale and complexity of the insurer's business, the outsourcing of one or more control functions may be appropriate for some insurers~~.

Comment [TmA2]: Deleted because included in 8.2.8. and 8.7

Special considerations for groups

~~8.0.7~~8.0.5 ~~Adequate governance, including risk management and internal controls, should be in place within the group.~~ Adequate risk management and internal controls at the group level, as well as at the legal entity level, is key to effective control and proper management of an insurance group. Group wide risks may affect legal entities within a group, while risks at the legal entity level could also have ramifications for the risk profile of the group as a whole, and (some or all) other entities within the group. Moreover, insurance groups, regardless of the organisational model, are required to comply with local laws and regulations, while also meeting the requirements applicable to groups. For this purpose, amongst other things, they need to have a strong risk and compliance culture at all levels[3].

Comment [TmA3]: Added, because only the responsibility of the supervisor was described.

~~8.0.8~~8.0.6 Supervisors should require and assess the establishment of comprehensive and consistent group governance. Effective control functions within a group are a core concern for supervisors. While

Comment [U14]: better distinction of the roles between different supervisors. Some of this new text comes from the Issues Paper.

[3] See Issues Paper, Approaches to Group Corporate Governance; impact on control functions, October 2014, para 49-50.

the group-wide supervisor is responsible for such assessments at the group level, the other involved supervisors undertake them on a legal entity basis. Assessing the effectiveness of the internal controls and risk management of the group as a whole should be done ~~This should be assessed by the supervisor~~ on a group-wide basis as well as on a legal entity basis. ~~–~~Appropriate supervisory cooperation and coordination is ~~required~~necessary to have a group-wide view and to enhance the assessment of the legal entities.

~~8.0.9~~ Groups may adopt different types of organisational ~~or~~ and operational structures for risk management and internal controls, depending on their management structure. ~~(referred to here as "management structures"), sometimes centralised, sometimes decentralised.~~ [4] ~~–~~The supervisor should take the management structure of the group into consideration in assessing ~~evaluating~~ its ~~governance~~risk management and internal controls. ~~Particularly when the management structure differs from the legal entity structure, it is not sufficient to address governance or risk only at the legal entity level. In such a case, i~~It is important that appropriate ~~governance~~ risk management and internal controls exist~~s~~ at group level and across the group, and that risks are properly ~~being identified, assessed,~~ monitored and managed at legal entity and ~~appropriately also~~ on a group-wide basis.

Comment [NM5]: The parts of this guidance that addressed Governance have been moved to 7.0.10. This guidance retains a more or less the similar message but with reference to Risk Management and Internal Controls, as topics for ICP 8.

~~*Supervisory and insurer responsibility*~~

Comment [TmA6]: Deleted as this applies to ICPs in general

~~8.0.10~~8.0.7 ~~The supervisor develops supervisory practices for the assessment of the insurer's systems of risk management and internal controls pursuant to this ICP. The ultimate responsibility, however, for the insurer having in place the necessary systems and functions for risk management and internal controls lies with the Board and Senior Management of the insurer.~~

Systems for risk management and internal controls

8.1 The supervisor requires the insurer to establish, and operate within, an effective ~~systems of~~ risk management system ~~and internal controls~~.

Comment [DH7]: We are suggesting separate standards on risk management and on internal controls and have therefore deleted "internal controls" from this standard. See new Standard 8.2 on internal controls.

Basic components of a risk management system

8.1.1 The risk management system is designed and operated to identify, assess, monitor, ~~manage~~ mitigate and report on all reasonably

[4] ~~For additional information on the variety of approaches to governance and management structures used within insurance groups and the different impact and demands those approaches can have on control functions, see the IAIS Issues Paper on Approaches to Group Corporate Governance; Impact on Control Functions of October 2014.~~

foreseeable material risks of the insurer in a timely manner. It takes into account the probability, potential impact and time ~~duration~~ horizon of risks.

8.1.2 ~~Subject to the nature, scale and complexity of the insurer, A~~an effective risk management system typically includes elements such as:

- a clearly defined and well documented risk management strategy, which includes a clearly defined risk appetite and ~~which~~ takes into account the insurer's overall business strategy ~~(as approved by the Board, and which will define the insurer's risk appetite on each business area)~~ and its business activities (including any business activities which have been outsourced);
- relevant objectives, key principles and proper allocation of responsibilities for dealing with risk across the business areas and ~~organisational~~business units of the insurer~~, including branches~~;
- ~~a clearly defined risk appetite approved by the Board in consultation with Senior Management;~~
- a ~~written~~ documented process defining the Board approval required for any deviations from the risk management strategy or the risk appetite and for settling any major interpretation issues that may arise;
- appropriate written policies that include a definition and categorisation of ~~reasonably foreseeable and relevant~~ material risks (by type) to which the insurer is exposed, and the levels of acceptable risk limits for each type of risk. ~~(such as underwriting, market, credit, liquidity, operational, (including outsourcing and conduct of business) and reputational risk, but also internal risks such as those arising from intra-group or related party pricing, transfers, transactions, outsourcing, etc.).~~ These policies describe~~fine~~ the risk standards and the specific obligations of employees and the businesses in dealing with risk, including ~~in respect of capital,~~ risk escalation and risk mitigation ~~(e.g. reinsurance, hedging)~~;
- suitable processes and tools (including stress testing and, where appropriate, models) for identifying, assessing, monitoring, ~~managing~~mitigating, and reporting on risks. Such processes should also cover ~~areas such as~~ contingency planning~~, business continuity and crisis management~~;
- ~~early warning or trigger system that allows a timely consideration and adequate response to treatment of material threats;~~

Comment [DH8]: The terminology "time horizon" is more prevalent in risk management than "time duration".

Comment [DH9]: Included this here to emphasise the fact that the risk appetite is part of the risk management strategy of an insurer.

Comment [TmA10]: Changed to be consistent: organisational only used for structures and 'business' used for 'units' or 'areas'

Comment [NM11]: See Glossary: the phrase "including branches" is unnecessary, as it is incorporated in the definition of the term "insurance legal entity" which is included in the term "Insurer".

Comment [NM12]: The section on risk appetite has been included in the first bullet point and then expanded on under "scoping and embedding".

Comment [DH13]: This is a start in bridging some of the gaps with ICP 16.

Comment [DH14]: Not all three terms are necessary. There seems to be a lot of overlap between these concepts. ICP 16 further talks about "continuity analysis". We would argue that crisis management and business continuity is a subset of contingency planning.

Comment [DH15]: This is to be moved to Scope and embedding. The "elements" which are listed here should not deal with functions (e.g. identifying, assessing, monitoring, managing or reporting), but rather stay focussed on the elements (strategies, policies, processes).

- regular reviews of the risk management system (and its components) to help ensure that necessary modifications and improvements are identified and made in a timely manner;
- ~~reporting on risks should be both to the Board and/or to operating units~~ Senior Management, ~~as appropriate~~, ~~using qualitative and quantitative indicators and action plans that can be effectively used;~~
- appropriate attention to other matters set out in ICP 16 Enterprise Risk Management for Solvency Purposes; and
- an effective risk management function.

Scope and embedding of the risk management system

8.1.3 The risk management system should at least cover underwriting and reserving, asset-liability management, investments, liquidity and concentration risk management, operational risk management, conduct of business, and reinsurance and other risk-mitigation techniques.

~~8.1.3~~8.1.4 The risk management system should be ~~integrated into the~~ aligned with its risk culture and embedded ~~of the insurer and~~ into the various business areas and units ~~of the insurer~~ with the aim of having the appropriate risk management practices and procedures embedded in the key operations and structures ~~of the insurer enterprise wide~~.

Identification

~~8.1.4~~8.1.5 The risk management system should take into account all reasonably foreseeable and relevant material risks to which the insurer is exposed, both at the ~~enterprise~~insurer ~~wide~~ and the individual business unit levels. This includes current and emerging risks.

Significant new or changed activities and products ~~of the insurer~~ that may increase an existing risk or create a new type of exposure should be subject to appropriate risk review and be approved by the Board and Senior Management.

~~8.1.5~~8.1.6

Assessment

8.1.7 Insurers should assess material risks both qualitatively and, where appropriate, quantitatively. Appropriate consideration should be given to a sufficiently wide range of outcomes, as well as to the appropriate tools and techniques to be used. The interdependencies

Comment [DH16]: Moved to Scope and embedding. The "elements" which are listed here should not deal with functions (e.g. identifying, assessing, monitoring, managing or reporting), but rather stay focussed on the elements (strategies, policies, processes).

Comment [NM17]: original 8.1.9

Comment [DH18]: This is a placeholder for ICP 16.1. GWG has brought the high-level concept in for now under a new guidance paragraph, but we can think about expanding it going forward with some of the guidance which falls under ICP 16.1. A lot of the guidance there may however be more suited for an applications paper.

of risks should also be analysed and taken into account in the assessments;

Monitoring

8.1.8 The risk management system should include early warnings or triggers that allows timely consideration of, and adequate response to, material risks.

Mitigation

8.1.9 The risk management system should include strategies and tools to mitigate against material risks.

Reporting

Risks and the overall assessment of risks should be reported to the Board and/or to Senior Management, as appropriate, using qualitative and quantitative indicators and effective action plans.

8.1.10 The insurer's documented risk escalation process should allow for reporting on risk issues within established reporting cycles and outside of them for matters of particular urgency.

Comment [NM19]: Original 8.1.7

8.1.11 The Board should have appropriate ways to carry out its responsibilities for risk oversight. ~~This includes having a~~The risk management policy should therefore cover~~on~~ the content, form and frequency of reporting that it expects on risk from Senior Management and each of the control functions. Any proposed activity that would go beyond the Board-approved risk appetite should be subject to appropriate review and require Board approval.

Comment [NM20]: Original 8.1.8

Risk Policies

~~8.1.6~~8.1.12 The insurer's risk policies should be written in a way to help employees understand their risk responsibilities. They should also help explain the relationship of the risk management system to the insurer's overall governance framework and to its corporate culture. The overall risk management policy of the insurer should outline how relevant and material risks are managed. Related policies should be established, either as elements of the risk management policy, or as separate sub-policies. At a minimum, these should include policies related to the risk appetite framework, an asset-liability management policy, an investment policy, and an underwriting risk policy.

Comment [DH21]: Incorporating ICP 16.4 and building in FSB RAF.

~~8.1.7~~8.1.13 Regular internal communications and training on risk policies should take place.

Changes to the risk management system

8.1.88.1.14 Both the Board and Senior Management should be attentive to the ~~potential~~ need to modify the risk management system in light of new internal or external circumstances.

Comment [NM22]: Original 8.1.10

8.1.98.1.15 Material changes to an insurer's risk management system should be documented and subject to approval by the Board. The reasons for the changes should be documented. Appropriate documentation should be available to internal audit, external audit and the supervisor for their respective assessments of the risk management system.

Comment [NM23]: Original 8.1.11

8.2 The supervisor requires the insurer to establish, and operate within, an effective system of internal controls

Basic components of an ~~i~~internal controls system

8.1.108.2.1 The internal controls system should ensure effective and efficient operations, adequate control of risks, prudent conduct of business, reliability of financial and non-financial information reported, both internally and externally, and compliance with laws, regulations, supervisory requirements and the ~~institutions~~insurer's internal rules and decisions. It should be designed and operated to assist the Board and Senior Management in the fulfilment of their respective responsibilities for oversight and management of the ~~company~~insurer. ~~The internal controls system provides them with reasonable assurance from a control perspective that the business is being operated consistently with the strategy and risk appetite set by the Board; agreed business objectives; agreed policies and processes; and applicable laws and regulations.~~[5]

Comment [NM24]: Original 8.1.12

Comment [TmA25]: Cf BCBS 113

Comment [TmA26]: Merged with 8.0.2 and partly deleted, because of duplication

8.2.2 The internal controls system should cover all units and activities of the insurer and should be an integral part of the daily activities of an insurer. The controls should form a coherent system, which should be regularly assessed and improved as necessary. Each individual control[6] of an insurer, as well as all its controls cumulatively, should be designed for effectiveness and operate effectively.

Comment [NM27]: Reworded original 8.1.14.

Comment [NM28]: from original 8.1.13

[5] ~~While risk management and internal controls are discussed separately in this document, some supervisors or insurers may use "internal controls" as an umbrella term to include risk management, internal audit, compliance, etc. The two terms are in fact closely related. Consensus on where the boundary lies between risk management and internal controls is less important than achieving, in practice, the objectives of each.~~

[6] Individual controls may be preventive (applied to prevent undesirable outcomes) or detective (to uncover undesirable activity). Individual controls may be manual (human), automated, or a combination ~~thereof~~ and may be either general or process or application specific. ~~Further classification of controls is sometimes used such as distinguishing between controls that apply to inputs or to outputs and between key and other controls.~~

8.2.3 An effective internal control system requires an appropriate control structure with control activities defined at every business level. Depending on the organisational structure of the insurer, business or other units should be primary responsible and accountable for establishing and maintaining adequate internal control policies and procedures. Independent control functions should monitor that these policies and procedures are complied with and should provide assurance on the quality and effectiveness of the internal controls system.[7]

8.2.4 ~~To provide additional checks and balances, s~~Some insurers have a designated person or function to support the advancement, coordination and/or management of the overall internal controls system on a more regular basis (such as an internal controls system manager~~ or similar~~). ~~At a minimum, the internal controls system should be designed and operated to provide reasonable assurance over the insurer's key business, IT and financial policies and processes, including accounting and financial reporting, and the related risk management and compliance measures in placeEach individual control [8] of an insurer, as well as all its controls cumulatively, should be designed for effectiveness and operate effectively.~~ An effective internal controls system typically includes :

Segregation of duties and prevention of conflicts of interest

- appropriate segregation of duties ~~where necessary~~ and controls to ensure such segregation is observed. This includes, amongst others, having sufficient distance between those accountable for a process or policy and those who check if for such a process or policy an appropriate control exists and is being applied. It also includes appropriate distance between those who design a control or operate a control and those who check if such a control is effective in design and operation;
- up-to-date policies regarding who can sign for or commit the insurer, and for what amounts, with corresponding controls, such as ~~the requirement~~practice that key decisions should be taken at least by two persons and the

Comment [TmA29]: CF BCBS para 35-41

Comment [TmA30]: Included old footnote 9 partly in footnote 7

Comment [NM31]: Parts taken from original 8.2.7

Comment [NM32]: Original 8.1.13

Comment [TmA33]: Included in new 8.1.11

Comment [TmA34]: moved to 8.1.11

Comment [TmA35]: all parts below under 8.2.4 are from original guidance **8.1.19** and somewhat amended

[7] This division of responsibilities between business, risk management and compliance and internal audit is typically referred to as the three lines of defence. The business is considered as the first line of defence, the control functions (other than internal audit) as the second line of defence, and internal audit as the third line of defence. The business is deemed to "own" the controls, and the other lines of defence are there to help ensure their application and viability. Whatever approach is used, it is important that responsibilities be clearly allocated to promote checks and balances and avoid conflicts of interest.[existing footnote moved]

~~[8] Individual controls may be preventive (applied to prevent undesirable outcomes) or detective (to uncover undesirable activity). Individual controls may be manual (human), automated, or a combination thereof and may be either general or process or application specific. Further classification of controls is sometimes used such as distinguishing between controls that apply to inputs or to outputs and between key and other controls.~~

practice of double or multiple signatures. Such policies and controls should be designed, among other things, to prevent any major transaction being entered into without appropriate governance review or by anyone lacking the necessary authority and to ensure that borrowing, trading, risk and other such limits are strictly observed. Such policies should foresee a role for control functions, for example by requiring for major matters the review and sign-off by Risk Management or Compliance, and/or approval by a Board level committee;

Policies and processes

- appropriate controls for ~~other~~ all key business processes and policies, including for major business decisions and transactions (including intra-group transactions), critical IT functionalities, access to databases and IT systems by employees, and important legal and regulatory obligations;
- policies on training in respect of controls, particularly for employees in positions of high trust or responsibility or involved in high risk activities;
- a centralised written inventory of insurer-wide key processes and policies and of the controls in place in respect of such processes and policies;

Information and communication

- appropriate controls to provide reasonable assurance over the accuracy and completeness of the insurer's books, records, and accounts and over financial consolidation and reporting, including the reporting made to the insurer's supervisors;
- adequate and comprehensive internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Information should be reliable, timely, accessible, and provided in a consistent format;
- information systems that cover all significant activities of the insurer, including contingency arrangements;
- effective channels of communication to ensure that all staff fully understand and adhere to the internal controls and their duties and responsibilities and that other relevant information is reaching the appropriate personnel;
- policies regarding escalation procedures;

Monitoring and review

- processes for regularly checking that the totality of all controls forms a coherent system and that this system works as intended; fits properly within the overall governance structure of the insurer; and provides an

Comment [TmA36]: BCBS paper on Internal Controls system, Principle 7

Comment [TmA37]: BCBS paper on Internal Controls system, Principle 8

Comment [TmA38]: BCBS paper on Internal Controls system, Principle 9

Comment [TmA39]: Cf BCBS 114

element of risk control to complement the risk identification, risk assessment, and risk management activities of the insurer. As part of such review, individual controls are monitored and analysed periodically to determine gaps and improvement opportunities with Senior Management taking such measures as are necessary to address these; and

- periodic testing and assessments (carried out by objective parties such as an internal or external auditor) to determine the adequacy, completeness and effectiveness of the internal controls system and its utility to the Board and Senior Management for controlling the operations of the insurer.

Responsibilities of the Board

8.1.118.2.5 ~~In fulfilling its responsibility in respect of the internal controls system, the Board reviews and approves the organisational and other measures regarding internal controls. The goal is a coherent system where the controls form a group-wide framework (from process or transactional level, to legal entity level, to group level) which can be regularly assessed and improved as necessary for maximum effectiveness.~~ The Board should have~~has~~ an overall understanding of the control environment across the various entities and businesses, and require~~s~~ Senior Management to ensure that for each key business process and policy, and related risks and obligations, there is an appropriate control.

8.1.128.2.6 In addition, the Board should ensure~~s~~ there is clear allocation of responsibilities within the insurer, with appropriate segregation, including in respect of the design, documentation, operation, monitoring and testing of internal controls. Responsibilities should be properly documented, such as in charters, authority tables, governance manuals or other similar governance documents [9]

8.1.138.2.7 The Board should determine~~s~~ which function or functions report to it or to any ~~existing~~ Board Committees in respect of the internal controls system.

Reporting

Comment [TmA40]: From original 8.1.14. Partly deleted, partly merged with new 8.2.2

Comment [NM41]: Original 8.1.15

Comment [NM42]: Original 8.1.16

Comment [TmA43]: taken from footnote 9 (deleted)

Comment [NM44]: Original 8.1.17

[9] ~~Appropriate segregation of duties is a fundamental building block of an internal controls system. Some companies in some jurisdictions allocate responsibilities according to the concept of "lines of defence" such as in considering management as the first line of defence, the control functions (other than internal audit) as the second line of defence, and internal audit as the third line of defence. Management is deemed to "own" the controls, and the other lines of defence are there to help ensure their application and viability. Whatever approach is used, it is important that responsibilities be allocated to promote checks and balances and avoid conflicts of interest. Responsibilities should be properly documented, such as in charters, authority tables, or other similar governance documents~~.

~~8.1.14~~8.2.8 Reporting on the internal controls system should cover matters such as:

- the strategy in respect of internal controls (such as responsibilities, target levels of compliance to achieve, validations and implementation of remediation plans);
- the stage of development of the internal controls system, including ~~the~~ its scope ~~that it covers~~, testing activity, and the performance against annual or periodic internal controls system goals being pursued;
- ~~information on resources (personnel, budget, etc.) being applied in respect of the internal controls system, including an analysis on the appropriateness of those resources in light of the nature, scale and complexity of the insurer's business, risks and obligations~~an assessment of how the various ~~organisational~~ business units ~~or major business areas of the insurer~~ are performing against internal control standards and goals; and
- control deficiencies, weaknesses and failures that have arisen or that have been identified (including any identified by the internal or external auditors or the supervisor) and the responses ~~thereto~~ (in each case to the extent not already covered in other reporting made to the Board).
- ~~Subject~~ controls at the appropriate levels so as to be effective, including at the process or transactional level, ~~at the entity level (whether legal entity or business area level), and in the case of groups, at the group level~~;

Comment [NM45]: Original 8.1.18

Comment [NM46]: Original 8.1.19

Comment [TmA47]: moved up to 8.2.4. keep only reporting issues in this part.

Control functions (general)

~~8.2~~8.3 The supervisor requires the insurer to have effective control functions with the necessary authority, independence and resources.

~~8.2.1~~8.3.1 As part of an effective system of risk management and internal controls, insurers have control functions, including for risk management, compliance, actuarial matters and internal audit. ~~While Senior Management has primary executive responsibility in respect of risk, compliance and related areas, specific control functions are essential for providing expertise, leadership, objectivity and independence where required on these subjects.~~ Control functions add to the governance checks and balances of the insurer and are a provide the necessary assurance~~source of support for~~ to the Board in the fulfilment of its ~~risk, compliance and control~~ oversight duties.

~~8.2.2 A control function should be led by a person of appropriate seniority and, expertise and integrity.~~

8.2.3 The appointment, performance assessment, remuneration, disciplining and dismissal of the head of each control function (other than the head of the internal audit function for which more stringent standards should apply) should be done with the approval of, or after consultation with, the Board or the relevant Board committee. While Senior Management may provide input, the appointment and the annual or other periodic performance assessment of the head of the internal audit function should be done by the Board (or its Chair or the Audit Committee) which solely determines his or her salary, bonus, and any promotions, demotions, or disciplinary actions.

Comment [NM48]: Original 8. 2.3 Edited and moved to new 8.3.5

8.2.48.3.2 The existence of control functions does not relieve the Board or Senior Management of their respective governance and related responsibilities.

8.2.5 Insurers should position each control function and its associated reporting lines into the insurer's organisational structure in a manner that enables such function to operate and carry out its responsibilities effectively.

8.2.68.3.3 The control functions (other than internal audit) should be subject to periodic internal or external review either by the insurer's internal auditor audit function (for control functions other than internal audit) or an objective external reviewer. The internal audit function should be subject to periodic review by an objective external reviewer.

8.2.7 To provide additional checks and balances, some insurers (particularly larger or more complex insurers) have a designated person or function to support the advancement, coordination and/or management of the overall internal controls system on a more regular basis (such as an internal controls system manager or similar). Unlike the internal or external auditor who may from time to time test certain controls or periodically opine formally on the existence or effectiveness of the internal controls system and who thus must have more operational distance, the internal controls system manager or similar is closer to the operations of the insurer and helps ensure that appropriate documented controls are in place for the appropriate areas and at the appropriate levels, locally and company wide.

Comment [MMT(49]: Original 8.2.7. **Parts MOVED to new 8.2.4**

8.2.88.3.4 Subject to supervisory approval where required, Aan insurer may combine certain control functions or outsource a control function in whole or in part with approval from the Board and the supervisor (where required) where appropriate in light of the nature, scale and complexity of the insurer's business, risks, and legal and regulatory obligations. In such cases, cases where an insurer combines or outsources a control function, or part thereof, the Board should satisfyies itself that this does not interfere with the function's independence, objectivity, or effectiveness. _The Board approves and also reviews periodically the effectiveness of such any arrangements for combining or outsourcing control functions,

including ~~by getting~~ obtaining an assessment ~~direct input~~ from the relevant control function(s).

Appointment and dismissal of heads of control functions

~~8.2.9~~8.3.5 The appointment, performance assessment, remuneration, disciplin~~ing~~ and dismissal of the head of each control function (other than the head of the internal audit function for which more stringent standards should apply) should be done with the approval of, or after consultation with, the Board or the relevant Board committee. ~~While Senior Management may provide input, the appointment and the annual or other periodic performance assessment of~~For the head of the internal audit function, the appointment, performance assessment, remuneration, discipline and dismissal should be done solely by the Board (or its Chair or the Audit Committee) ~~which solely determines his or her salary, bonus, and any promotions, demotions, or disciplinary actions~~.

8.3.6 The insurer should notify the supervisor ~~the~~ the reasons for dismissals of heads of control functions ~~to the supervisor~~.

Authority and independence of control functions

~~8.2.10 Each control function should have the authority and independence necessary to be effective in fulfilling its duties and attaining its goals.~~

8.3.7 The Board should ~~set or~~ approve the authority and responsibilities of each control function to allow each control function to have the authority and independence necessary to be effective.

~~8.2.11~~8.3.8 The authority and responsibilities of each control function should be set out in writing and made part of, or referred to in, the governance documentation of the insurer. The head of each control function should periodically review such document and submit suggestions for any changes to Senior Management and the Board for approval, where appropriate.

8.3.9 A control function should be led by a person of appropriate level of authority.~~seniority and expertise .~~ The head of the control function should not have ~~direct~~ operational business line responsibilities ~~and should not report to Senior Management who has direct business line responsibilities~~.

8.3.10 Insurers should organise ~~position~~ each control function and its associated reporting lines into the insurer's organisational structure in a manner that enables such function to operate and carry out ~~its~~their roles effectively. This includes formal reporting obligations to the Senior Management and the right of direct access to the Board or the relevant Board committee. ~~The head of the control function~~

Comment [NM50]: Added a guidance about information to the supervisor about dismissal of a control function. See 8.6.11/9.6.12

Comment [NM51]: Original 8.2.3

Comment [NM52]: Original 8.2.9

Comment [NM53]: Original 8.2.10

Comment [NM54]: Original 8.2.2

Comment [NM55]: 8.3.7. / 8.3.8 are better placed under resources and qualifications?

Comment [NM56]: Moved down to end of 8.3.9.

Comment [NM57]: From Original 8.2.5

~~should not report to Senior Management who has direct business line responsibilities~~.

~~8.2.12~~8.3.11 Notwithstanding the possibility for insurers to combine certain control functions, ~~as described in Guidance 8.2.8,~~ a control function should ~~'s~~ be sufficiently independen~~tce~~ from Senior Management and from other functions ~~should be sufficient~~ to allow its staff to:

- serve as a ~~further~~ component of the insurer's checks and balances;
- provide an objective perspective on strategies, issues, and potential violations related to their areas of responsibility; and
- implement or oversee the implementation of corrective measures where necessary.

~~8.2.13~~8.3.12 Each control function should avoid conflicts of interest. Where any conflicts remain and cannot be resolved with Senior Management, these should be brought to the attention of the Board for resolution.

8.3.13 Each control function should have the authority to communicate on its own initiative with any employee and to have unrestricted access to ~~such~~ information in any business unit that~~as~~ it needs to carry out its responsibilities. The control functions should have the right to conduct investigations of possible breaches and to request assistance from specialists within the insurer, e.g. legal and internal audit, or engage external specialists to perform the task.

The control functions should be free to report to Senior Management or the Board on any irregularities or possible breaches disclosed by its investigations, without fear of retaliation or disfavour from management. ~~In addition, control functions should have appropriate access to Senior Management.~~

Comment [NM58]: From original 8.2.14

Resources and qualifications of the control functions

Comment [NM59]: This part was below Board access and qualifications. Moved up.

~~8.2.14~~8.3.14 Each control function should have the resources necessary to fulfil its responsibilities and achieve the specific goals in its areas of responsibility. This includes qualified staff and appropriate IT/management information systems. The function should be organized in an appropriate manner ~~appropriate~~ to achieve its goals.

~~8.2.15~~8.3.15 The head of each control function should review regularly ~~with Senior Management~~ the adequacy of the function's resources and request adjustments from the Senior Management as necessary. Where the head of ~~each~~ a control function ~~he or she~~ has a major difference of opinion with Senior Management on the ~~amount of~~ resources needed, ~~such person~~the head of the control function

should bring the issue to the Board or relevant Board Committee for resolution.

~~8.2.16~~8.3.16 Persons who perform control functions should ~~possess the necessary integrity, experience, skills and knowledge~~be suitable ~~required~~ for their role ~~specific position they exercise~~ and meet any applicable professional qualifications and standards. Higher expectations apply to the head of each control function. ~~To ensure that p~~Persons who perform control functions should receive regular training relevant to their role to remain up to date on the developments and techniques related to their areas of responsibility~~, they should receive regular training relevant to their field and areas of responsibilities~~.

Board access and reporting by the control functions; Board assessment of control functions

Comment [NM60]: Part below was previously above resources and qualifications – moved down for better flow.

~~8.2.17~~8.3.17 The Board should grant the head of each control function the authority and responsibility to report periodically to it or one of its committees. The Board should determine the frequency and depth of such reporting so as to permit timely and meaningful communication and discussion of material matters. The reporting should include, among other things:

- information as to the function's strategy and longer term goals and the progress in achieving these;
- annual or other periodic operational plans describing shorter term goals and the progress in achieving these; and
- resources (such as personnel, budget, etc.), including an analysis on the adequacy of these resources.

~~8.2.18~~ In addition to periodic reporting, the head of each control function should have the opportunity to communicate directly and to meet periodically (without the presence of management) with the chair of any relevant Board committee (e.g. Audit or Risk Committee) and/or with the Chair of the full Board.

~~8.2.19~~8.3.18 The Board should periodically assess the performance of each control function. This may be done by the full Board, by the Chair of the Board, by the relevant Board committee ~~of the Board to which the head of the control function reports,~~ or by the Chair of ~~such~~ the relevant Board committee.

Risk management function

8.4 The supervisor requires the insurer to have an effective risk management function capable of assisting the insurer to

- **identify, assess, monitor, ~~manage~~ mitigate and report on its key risks in a timely way; and**
- **~~to~~ promote and sustain a sound risk culture.**

~~8.2.20~~8.4.1 A robust risk management function that is well positioned, resourced and properly authorised and staffed is an essential element of an effective risk management system. Within some insurers, and particularly at larger or more complex ones, the risk management ~~such a~~ function is typically led by a Chief Risk Officer ~~or similar~~.

Access and reporting to the Board by the risk management function

~~8.2.21~~8.4.2 The risk management function should have access ~~to~~ and provide written reports to the Board as required by the Board, typically on matters such as:

- an assessment of risk positions and risk exposures and steps being taken to manage them;
- an assessment of changes in the insurer's risk profile relative to risk appetite;
- where appropriate, an assessment of pre-defined risk limits;
- where appropriate, risk management matters in relation to strategic affairs such as corporate strategy, mergers and acquisitions and major projects and investments;
- an assessment of risk events and the identification of appropriate remedial actions.

Comment [DH61]: Taken from FSB guidance on Risk appetite

~~8.2.22~~8.4.3 The head of the risk management function should have the authority and obligation to inform the Board promptly of any circumstance that may have a material effect on the risk management system of the insurer.

Main activities of the risk management function

~~8.2.23~~8.4.4 The risk management function should establish, implement and maintain appropriate mechanisms and activities to:

- assist the Board and Senior Management in carrying out their respective responsibilities, including by providing specialist analyses and performing risk reviews;
- identify the individual and aggregated risks (actual, emerging and potential) the insurer faces;
- assess, aggregate, monitor and help manage and otherwise address identified risks effectively; this includes assessing the insurer's capacity to absorb risk with due

regard to the nature, probability, duration, correlation and potential severity of risks;

- gain and maintain an aggregated view of the risk profile of the insurer both at a legal entity and/or ~~at the~~ group-wide level;
- establish a forward-looking assessment of the risk profile;
- evaluate the internal and external risk environment on an on-going basis in order to identify and assess potential risks as early as possible. This may include looking at risks from different perspectives, such as by territory or by line of business;
- consider risks arising from remuneration arrangements and incentive structures;
- conduct regular stress testing and scenario analyses as defined in ICP 16 Enterprise Risk Management for Solvency Purposes;
- regularly provide written reports to Senior Management, Key Persons in Control Functions and the Board on the insurer's risk profile and details on the risk exposures facing the insurer and related mitigation actions as appropriate;
- document and report material changes affecting the insurer's risk management system to the Board to help ensure that the framework is maintained and improved; and
- conduct regular assessments of the risk management function and the risk management system and implement or monitor the implementation of any needed improvements.

Compliance function

~~8.3~~8.5 **The supervisor requires the insurer to have an effective compliance function capable of assisting the insurer to meet its legal, ~~and~~ regulatory and supervisory obligations and internal policies and to promote and sustain a corporate culture of compliance and integrity.**

8.5.1 The compliance function is responsible for promoting and monitoring that an insurer operates with integrity and in compliance with applicable laws, regulations, and internal policies. The compliance function has a broader role than merely a legal role ~~function~~ for monitoring compliance with laws and regulations; monitoring compliance with internal policies and promoting and sustaining a compliance culture within the insurer are equally important aspects of this control function.

Comment [AF62]: Taken from FSB

Comment [DH63]: GWG agreed to leave this wording in for now… to reconsider when reviewing ICP 16.

Comment [NM64]: Or "function"?

Comment [U165]: This is based on the recommendation from the SAPR -- made a slight addition to the standard to reinforce that the compliance function looks at things that are both external and internal to the company.

8.3.18.5.2 ~~The Board adopts a code of conduct or takes other appropriate means to commit the insurer to comply with all applicable laws, regulations, supervisory decisions, and internal policies, and conduct its business ethically and responsibly.~~Compliance starts at the top. The Board is ultimately responsible for establishing standards for honesty and integrity throughout the insurer and for creating an effective corporate culture that emphasises them. This should include a code of conduct or other appropriate mechanism as evidence of the insurer's commitment to comply with all applicable laws, regulations, supervisory decisions, and internal policies, and conduct its business ethically and responsibly.

Comment [NM66]: Original 8.4.1

8.3.28.5.3 As part of this commitment, the insurer has in place a robust and well positioned, resourced and properly authorised and staffed compliance function. Within some insurers, particularly larger or more complex ones, such a function is typically led by a Chief Compliance Officer or similar.

Board access and reporting of the compliance function

8.3.38.5.4 The compliance function should have access ~~to~~ and provide written reports to the Board on matters such as:

- an assessment of the key compliance risks the insurer faces and the steps being taken to address them;
- an assessment of how the various parts of the insurer (e.g. divisions, major business units, product areas~~, etc.~~) are performing against compliance standards and goals;
- any compliance issues involving management or persons in positions of major responsibility within the insurer, and the status of any associated investigations or other actions being taken;
- material compliance violations or concerns involving any other person or unit of the insurer and the status of any associated investigations or other actions being taken;
- material fines or other disciplinary actions taken by any regulator or supervisor in respect of the insurer or any employee.

8.3.48.5.5 The head of the compliance function should have the authority and obligation to ~~promptly~~ inform promptly the Chair of the Board directly in the event of any major non-compliance by a member of management or a material non-compliance by the insurer with an external obligation if in either case he or she believes that Senior Management or other persons in authority at the insurer are not taking the necessary corrective actions and a delay would be detrimental to the insurer or its policyholders.

Main activities of the compliance function

~~8.3.5~~8.5.6 The compliance function should establish, implement and maintain appropriate mechanisms and activities to:

- promote and sustain an ethical corporate culture that values responsible conduct and compliance with internal and external obligations; this includes communicating and holding training on an appropriate code of conduct or similar that incorporates the corporate values of the insurer, aims to promote a high level of professional conduct and sets out the key conduct expectations of employees;
- identify, assess, report on and address key legal and regulatory obligations, including obligations to the insurer's supervisor, and the risks associated therewith; such analyses should use risk and other appropriate methodologies;
- ensure the insurer monitors and has appropriate policies, processes and controls in respect of key areas of legal, regulatory and ethical obligation;
- hold regular training on key legal and regulatory obligations particularly for employees in positions of high responsibility or who are involved in high risk activities;
- facilitate the confidential reporting by employees of concerns, shortcomings or potential or actual violations in respect of insurer internal policies, legal or regulatory obligations, or ethical considerations; this includes ensuring there are appropriate means for such reporting;
- address compliance shortcomings and violations, including ensuring that adequate disciplinary actions are taken where appropriate and any necessary reporting to the supervisor or other authorities is made; and
- conduct regular assessments of the compliance function and the compliance systems and implement or monitor needed improvements.

~~8.3.6~~8.5.7 Additionally, the compliance function should focus on areas which could pose a higher level of risk to the insurer such as fraud or other financial crime, misleading information to customers, and conflicts of interest.

Comment [U167]: In reviewing the Basel Cmte's work, this seemed like a good point that we had not covered.

Actuarial function

~~8.4~~8.6 **The supervisor requires that there is an effective actuarial function capable of evaluating and providing advice to the insurer regarding, at a minimum, technical provisions, premium and pricing activities, capital adequacy,**

reinsurance and compliance with related statutory and regulatory requirements.

~~8.4.1~~8.6.1 A robust actuarial function that is well positioned, resourced and properly authorised and staffed is essential for the proper operation of the insurer. It plays a key role as part of the insurer's overall system of risk management and the internal control framework.

~~8.4.2 The supervisor should have or have access to the appropriate skills, knowledge and resources to enable it to critically assess the work of an insurer's actuarial function.~~

Comment [xx68]: GWG suggests to move this to under ICP 9 or ICP 2.

Board access and reporting of the actuarial function

~~8.4.3~~8.6.2 The actuarial function should have access to and periodically report to the Board on matters such as:

- any circumstance that may have a material effect on the insurer from an actuarial perspective;
- the adequacy of the technical provisions and other liabilities;
- distribution of profits ~~or dividends awarded~~ to participating policyholders;
- stress testing and capital adequacy assessment with regard to the prospective solvency position of the insurer; and
- any other matters as determined by the Board.

~~8.4.4~~8.6.3 Written reports on actuarial evaluations should be made to the Board, Senior Management, or other Key Persons in Control Functions or the supervisor as necessary or appropriate or as required by legislation.

Main activities of the actuarial function

~~8.4.5~~8.6.4 ~~The actuarial function should carry out such activities as are needed to evaluate and provide advice to the insurer in respect of technical provisions, premium and pricing activities and compliance with related statutory and regulatory requirements.~~ The actuarial function carries out all activities which are needed to evaluate~~s~~ and provide~~s~~ advice to the insurer on matters such as:

Comment [NM69]: Original 8.5.5. Parts deleted based on comments from AAA.

- the insurer's insurance liabilities, including policy provisions and aggregate claim liabilities, as well as determination of reserves for ~~actuarial and~~ financial risks;
- asset liability management with regards to the adequacy and the sufficiency of assets and future revenues to cover

the insurer's obligations to policyholders and capital requirements, as well as other obligations or activities;

- the insurer's investment policies and the valuation of assets;
- an insurer's solvency position, including a calculation of minimum capital required for regulatory purposes and liability and loss provisions;
- an insurer's prospective solvency position by conducting capital adequacy assessments and stress tests under various scenarios, and measuring their relative impact on assets, liabilities, and actual and future capital levels;
- risk assessment and management policies and controls relevant to actuarial matters or the financial condition of the insurer;
- the fair treatment of policyholders with regard to distribution of policy dividends or other benefits, consistent with policyholders' reasonable expectations;
- the adequacy and soundness of underwriting policies;
- the development, pricing and assessment of the adequacy of reinsurance arrangements;
- product development and design, including the terms and conditions of insurance contracts and pricing, along with estimation of the capital required to underwrite the product;
- the sufficiency, accuracy and quality of data, the methods and the assumptions used in the calculation of technical provisions; ~~and~~
- ~~risk modelling in the ORSA~~ the research, development, validation and use of internal models for internal actuarial or financial projections, or for solvency purposes as in the ORSA; ~~and~~
- any other actuarial or financial matters determined by the Board.

~~8.4.6~~8.6.5 Where required, the actuarial function may also provide to the ~~relevant~~ supervisor certifications on the adequacy, reasonableness and/or fairness of premiums (or the methodology to determine the same) and certifications or statements of actuarial opinion.

~~8.4.7~~8.6.6 The supervisor should clearly define when such certifications or statements of actuarial opinion need to be submitted to the supervisor ~~filed~~. When these are required to be submitted ~~filed~~, the supervisor should also clearly define both the qualifications of those permitted to certify or sign such statements and the minimum contents of such an opinion or certification.

Appointed actuary

~~8.4.8~~8.6.7 Some jurisdictions may require an "appointed actuary," "statutory actuary," or "responsible actuary" (~~hereinafter~~ referred to here as an "Appointed Actuary") to perform certain functions, such as determining or providing advice on an insurer's compliance with regulatory requirements for certifications or statements of actuarial opinion. The tasks and responsibilities of the Appointed Actuary should be clearly defined and should not limit or restrict the tasks and responsibilities of other individuals performing actuarial functions.

~~8.4.9~~8.6.8 The insurer should be required~~, at a minimum,~~ to report the Appointed Actuary's appointment to the supervisor.

~~8.4.10~~8.6.9 The Appointed Actuary should not hold positions within or outside of the insurer that may create conflicts of interest or compromise his or her independence. If the Appointed Actuary is not an employee of the insurer, the Board should determine whether the external actuary has any potential conflicts of interest, such as if his or her firm also provides auditing or other services to the insurer. If any such conflicts exist, the Board should subject them to appropriate controls or choose another Appointed Actuary~~order other arrangements~~.

8.6.10 If an Appointed Actuary ~~resigns or~~ is replaced, the insurer should notify the supervisor and give the reasons for the ~~resignation or~~ replacement. In some jurisdictions, such a notification includes ~~a~~ statements from both the insurer and the former Appointed Actuary as to~~of~~ whether there were any disagreements with the former Appointed Actuary over the content of the actuary's opinion on matters of risk management, required disclosures, scopes, procedures, or data quality, and whether or not any such disagreements were resolved to the former Appointed Actuary's satisfaction.

~~8.4.11~~8.6.11 In some jurisdictions, the Appointed Actuary also has the obligation to notify the supervisor if he or she resigns for reasons connected with his or her duties as an Appointed Actuary or with the conduct of the insurer's business and give the reasons for resigning. The Appointed Actuary should also notify the supervisor and give the reasons for it if his or her appointment is revoked by the insurer.

~~8.4.12~~8.6.12 The supervisor should have the authority to require an insurer to replace an Appointed Actuary when such person fails to adequately perform required functions or duties, is subject to conflicts of interest or no longer meets the jurisdiction's eligibility requirements.

Internal audit function

8.58.7 **The supervisor requires the insurer to have an effective internal audit function capable of providing the Board with independent assurance in respect of the quality and effectiveness of the insurer's governance framework, including its risk management and internal controls.**

8.5.18.7.1 Part One of the oversight roles of the Board is to ensure that the information provided by the there are means for it to receive independent assurance from an internal audit function allows them to effectively validate the performance of the internal control system. that is not operationally involved in the business and is not subject to any conflicts of interest.

8.5.28.7.2 The internal audit function should provide independent assurance to the Board through general and specific audits, reviews, testing and other techniques in respect of matters such as:

- the overall means by which the insurer preserves its assets and those of policyholders, and seeks to prevent fraud, misappropriation or misapplication of such assets;
- the reliability, integrity and completeness of the accounting, financial and risk reporting and management information, as well as the capacity and adaptability of and IT architecture to provide that information in a timely manner to the Board and Senior managementsystems;
- the design and operational effectiveness of the insurer's individual controls in respect of the above matters, as well as of the totality of such controls (the internal controls system);
- other matters as may be requested by the Board, Senior Management, or the supervisor or the external auditor; and
- other matters which the internal audit function determines should be reviewed to fulfil its mission, in accordance with its charter, terms of reference or other documents setting out its authority and responsibilities.

Authority and independence of the internal audit function

8.5.38.7.3 To help ensure objectivity, the internal audit function is independent from management and is not involved operationally in the business. The internal audit function's ultimate responsibility is to the Board, not management. To help ensure independence and objectivity, the internal audit function should be free from conditions that threaten its ability to carry out its responsibilities in an unbiased manner. In carrying out its tasks, the internal audit function forms its judgments independently. If necessary, the internal audit function should consider the need to supplement its own assessment with third party expertise in order to make objective and independent decisions.

Comment [NM70]: Original 8.6

Comment [xx71]: See glossary

Comment [NM72]: Noted this in the FSB's guidance on risk culture.

~~8.5.4~~8.7.4 The Board should grant suitable authority to the internal audit function, including the authority to:

- access and review any records or information of the insurer which the internal audit function deems necessary to carry out an audit or other review;
- undertake on the internal audit function's initiative a review of any area or any function consistent with its mission;
- require an appropriate management response to an internal audit report, including the development of a suitable remediation, mitigation or other follow-up plan as needed; and
- decline doing an audit or review, or taking on any other responsibilities requested by management, if the internal audit function believes this is inconsistent with its mission or with the strategy and audit plan approved by the Board. In any such case, the internal audit function should inform the Board or the Audit Committee and seek ~~its~~ their guidance.

Board access and reporting of the internal audit function

~~8.5.5~~8.7.5 The head of the internal audit function reports to the Board (or to any member who is not part of the management) or to the Audit Committee if one exists (or its Chair). In its reporting, the internal audit function should cover matters such as:

- the function's annual or other periodic audit plan, detailing the proposed areas of audit focus;
- any factors that may be adversely affecting the internal audit function's independence, objectivity or effectiveness;
- material findings from audits or reviews conducted; and
- the extent of management's compliance with agreed upon corrective or risk mitigating measures in response to identified control deficiencies, weaknesses or failures, compliance violations or other lapses.

~~8.5.6~~8.7.6 In addition to periodic reporting, the head of internal audit should be authorised to communicate directly, and meet periodically, with the head of the Audit Committee or the Chair of the Board without management present.

Main activities of the internal audit function

~~8.5.7~~8.7.7 The audit function should carry out such activities as are needed to fulfil its responsibilities. These activities include among others:

- establishing, implementing and maintaining a risk-based audit plan to examine and evaluate ~~general or specific areas, including on a preventive basis~~ alignment of the ~~institutions~~insurer's ~~'~~ systems and processes with their risk culture;
- reviewing and evaluating the adequacy and effectiveness of the insurer's policies and processes and the documentation and controls in respect of these, on a legal entity and group-wide basis and on an individual subsidiary, business unit, business area, department or other organisational unit basis;
- reviewing levels of compliance by employees, third parties and organisational units with laws and regulations (including requirements from supervisors), established policies, processes and controls, including those involving reporting;
- evaluating the reliability, ~~and~~ integrity and effectiveness of management information systems and processes and the means used to identify, measure, classify and report such information;
- ensuring that ~~the~~ identified risks ~~and the agreed actions to address them are accurate and current~~ are effectively addressed by the internal control framework~~;~~
- evaluating the means of safeguarding insurer and policyholder assets and, as appropriate, verifying the existence of such assets and the required level of segregation in respect of insurer and policyholder assets;
- monitoring and evaluating governance processes;
- monitoring and evaluating the effectiveness of the ~~organisation's~~ insurer's control functions, particularly ~~in their role as~~ the insurers' second line of defence (i.e. risk management and compliance); and
- coordinating with the external auditors and, to the extent requested by the Board and consistent with applicable law, evaluating the quality of performance of the external auditors.~~; and~~
- ~~conducting regular assessments of the internal audit function and audit systems and incorporating needed improvements~~.

~~8.5.8~~8.7.8 In carrying out the above tasks, the internal audit function should ensure all material areas of risk and obligation of the insurer are subject to appropriate audit or review over a reasonable period of time. Among these areas are those dealing with:

Comment [q73]: The Board should be directly responsible for this activity The functions should not assess themselves. (The same issue was raised in connection with the corresponding drafting in ComFrame – and amended).

- market, underwriting, credit, liquidity, operational, conduct of business, ~~and~~ as well as reputational issues derived from exposure to those risks~~risk~~;
- accounting and financial policies and whether the associated records are complete and accurate;
- extent of compliance by the insurer with applicable laws, regulations, rules and directives from all relevant jurisdictions;
- intra-group transactions, including intra-group risk transfer and internal pricing;
- adherence by the insurer to the insurer's remuneration policy;
- the reliability and timeliness of escalation processes and reporting systems, including whether there are confidential means for employees to report concerns or violations and whether these are properly communicated, offer the reporting employee adequate protection from retaliation, and result in appropriate follow up; and
- the extent to which any non-compliance with internal policies or external legal or regulatory obligations is documented and appropriate corrective or disciplinary measures are taken including in respect of individual employees involved.

~~8.5.9~~8.7.9 Subject to applicable laws on record retention, the internal audit function should keep careful records of all areas and issues reviewed so as to provide evidence of these activities over time.

Outsourcing of material activities or functions ~~or activities~~

~~8.6~~8.8 **The supervisor requires the insurer to retain at least the same degree of oversight of, and accountability for, any outsourced material activity or function (such as a control function) as applies to non-outsourced activities or functions.**

~~8.6.1~~8.8.1 ~~In general, o~~Outsourcing~~, whether to external parties or within the same insurance group,~~ should not materially increase risk to the insurer or materially adversely affect the insurer's ability to manage its risks and meet its legal and regulatory obligations.

~~8.6.2~~8.8.2 The Board and Senior Management remain responsible in respect of functions or activities that are outsourced.

~~8.6.3~~8.8.3 The supervisor should require the Board ~~of an insurer~~ to have review and approval processes~~approve~~ for outsourcing of any material activity or function ~~or activity~~ and to verify, before approving, that there was an appropriate assessment of the risks, as well as an

Comment [NM74]: Original 8.7. No change

Comment [NM75]: Refer to Glossary **See proposed new defintion of Outsourcing**:
"An arrangement between an insurer and a service provider for the latter to perform a process, service or activity which would otherwise be performed by the insurer itself. In the case of an insurance group, outsourcing could be either external or internal."

Comment [NM76]: original 8.7.7

assessment of the ability of the insurer's risk management and internal controls to ~~effectively~~ manage them effectively in respect of business continuity ~~of such outsourcing, including in respect of business continuity and that such outsourcing is subject to appropriate controls~~. The assessment should take into account to what extent the insurer's risk profile and business continuity could be affected by the outsourcing arrangement.

~~8.6.4~~8.8.4 The supervisor should require insurers which outsource any material ~~function or~~ activity or function to have in place an appropriate policy for this purpose, setting out the internal review and approvals required and providing guidance on the contractual and other risk issues to consider. This includes considering limits on the overall level of outsourced activities at the insurer and on the number of activities that can be outsourced to the same service provider. Because of the particularly important role that ~~control functions and~~ control activities and control functions play in an insurer's governance system, the supervisor should consider issuing additional requirements for their outsourcing or dedicating more supervisory attention to any such outsourcing.

~~8.6.5~~8.8.5 Outsourcing relationships should be governed by written contracts that clearly describe all material aspects of the outsourcing arrangement, including the rights, responsibilities and expectations of all parties. When entering into or varying an outsourcing arrangement, the Board and Senior Management should consider, among other things:

- how the insurer's risk profile will be affected by the outsourcing;
- the service provider's governance, risk management and internal controls and its ability to comply with applicable laws and with regulations;
- the service providers' service capability and financial viability; and
- succession issues to ensure a smooth transition when ending or varying an outsourcing arrangement.

~~8.6.6~~8.8.6 In choosing an outsourcing provider, the Board or Senior Management should be required to satisfy themselves as to the expertise, knowledge and skills~~experience~~ of such provider.

~~8.6.7~~8.8.7 Outsourcing arrangements should be subject to periodic reviews. Periodic report~~sing thereon~~ should be made to management and the Board. ~~The Board and Senior Management remain responsible in respect of functions or activities that are outsourced.~~

~~*Supervisory review*~~

Comment [NM77]: original 8.7.3

Comment [NM78]: Original 8.7.6

Comment [NM79]: Deleted from ICP 8. Suggest that Supervisory Review issues be covered in ICP 9. This relates to a SAPR recommendation made on 8.6, but it seemed applicable to all the control functions so suggest placing it here. Suggest to delete as this seemed better set out in ICP 9.

~~In assessing the insurer's systems of risk management and internal controls, the supervisor should review outsourced activities and functions at the same level that such activities and functions would be reviewed if they were done internally by the insurer. Such an assessment should be performed on an ongoing basis rather than only in response to supervisory concerns or action.~~

Comment [U180]: Added in response to the SAPR recommendation.