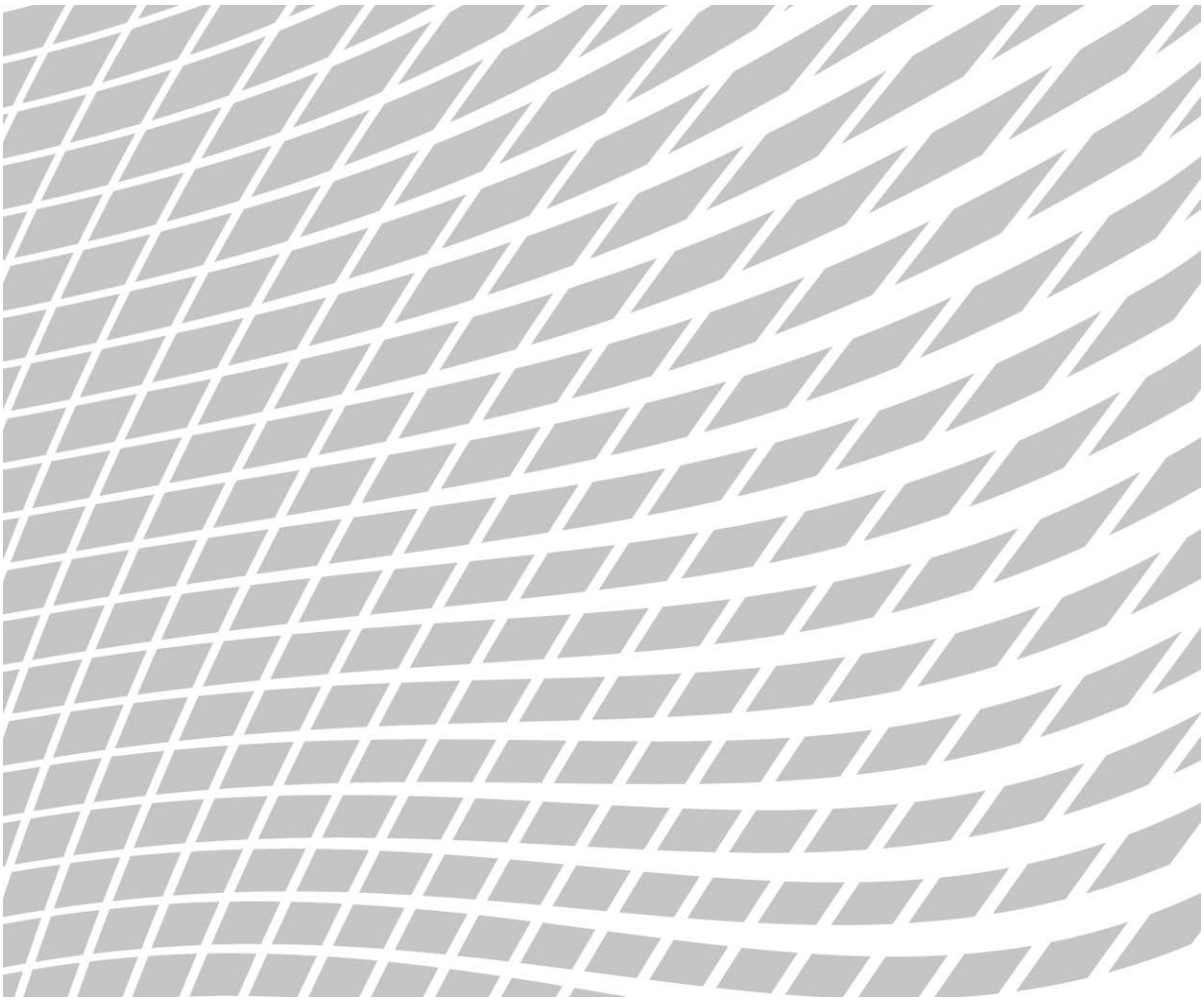
Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

5 April 2013

Governance, Risk Management and Internal Control Systems at Swiss Insurers

Observations from the Second Swiss Qualitative Assessment (SQA II)



Einsteinstrasse 2, 3003 Bern
Phone +41 (0)31 327 91 00, Fax +41 (0)31 327 91 01
www.finma.ch

A332785/GB-V/V-SQA

Table of contents

SUMMARY OF MAIN OBSERVATIONS

1. Positive maturation trend is observable among reviewed insurers in many, though not all, areas of governance, risk management and internal controls (CG/RM/ICS).
2. Progress, however, remains uneven across insurers.
3. Boards of Directors (BoD) show more awareness of their duty to provide oversight of Management and of risks. But there are questions on a) whether their informational needs are fully being met and b) their time availability.
4. There remain improvement needs in respect of a) the risk appetite framework and specific risk limits, b) risk governance, and c) the scope and operation of the Internal Controls System.
5. Compliance sensitivity is increasing. But there are remaining shortcomings in the structure and effective operation of Compliance Functions.
6. There are weaknesses in a) the governance and oversight of outsourcing and b) training employees on risk and compliance topics.
7. Insurers are not sufficiently measuring the effectiveness of their CG/RM/ICS efforts.
8. At some insurers there may be an underinvestment in the CG/RM/ICS areas.
9. Low interest rates, market instability, and compliance challenges are the top common risks facing insurers, as seen by their Control Functions.
10. For Control Functions, the top risks they believe they face as functions relate primarily to resources, know-how, and IT/modelling-related needs.

Glossary

BoD	Board of Directors
Control Functions	The internal audit, risk management, compliance and actuarial functions of an Insurer
CEO	Chief Executive Officer
CG	Corporate Governance
CRO	Chief Risk Officer
Group	Insurers supervised by FINMA as a Group, as well as insurers with large operations in Switzerland which are part of a non-Swiss insurance group
ICS	Internal Controls System
insurer	As used here, the term refers to an insurer or reinsurer, whether a Group or a Solo
insurers	Unless otherwise indicated, “insurers” refers to those insurers reviewed under SQA II
Key Risk Takers	Individuals who due to their position, authority, access to information, or nature of activities can affect the risk profile of the insurer
Management	A general reference to senior management at a company including but beyond the MB.
MB	Management Board, Executive Committee or similar highest-level management body
RM	Risk Management
Solo	An Insurer which does not belong to a Group, as defined above
SQA	Swiss Qualitative Assessment

A. Introduction

This report summarizes FINMA's key observations from the second Swiss Qualitative Assessment (SQA II) carried out primarily in 2012.

Consistent with FINMA's risk prioritisation, SQA II did not cover all insurers but those in the three highest risk categories under FINMA's supervisory approach (including all Groups), as well as additional insurers selected from the next risk category.

The observations in this report are based on FINMA's analyses of the SQA II submissions by these insurers and further exchanges and interactions with them. These included in some cases personal risk dialogs with members of the Board of Directors, senior management, heads of Control Functions, and other key company personnel. The assessments also take into account information gained by FINMA through its regular supervision of insurers.

Progress made by the reviewed insurers since their SQA II assessment by FINMA is not reflected in this report.

The next SQA (SQA III) is currently foreseen for early 2015.

B. SQA II Basis and Goals

FINMA considers corporate governance (CG), risk management (RM) and the internal controls system (ICS) as indispensable components for the sound management of a company.[1] Together with FINMA's on-going regular supervision, the SQA is a principal instrument for FINMA fulfilling its duty of oversight of insurers in these areas.

A central focus in SQA II has been the insurer's risk and governance culture and the interplay of its various organs. This includes the dynamics between the board of directors (BoD), Management and the Control Functions and the effectiveness of the systems, processes, and controls in place.

[1] Since the revision of the Swiss Federal Act on the Supervision of Insurance Companies in 2004 (entered into force 1 January 2006), insurers in Switzerland have been required to be in alignment with the CG/RM/ICS requirements and principles of this Act (Insurance Supervision Act [ISA]; SR 961.01; for supervisory practice, please refer to in FINMA-Circ. 08/32 and 08/35). See also FINMA Newsletter 17 (2010) http://www.finma.ch/e/finma/publikationen/Lists/ListMitteilungen/Attachments/17/finma-mitteilung-17-2010-e.pdf.

SQA II complements the quantitative focus of the Swiss Solvency Test (SST). It helps complete FINMA's understanding of an insurer's risk profile by providing insights on the nature and effectiveness of the qualitative measures an insurer is taking. Together with other supervisory information, these insights assist FINMA in formulating the risk rating for each insurer under FINMA's supervisory categories and the degree of supervisory intensity needed. They also help identify specific issues that may require immediate supervisory action.

SQA II is also designed to bring benefit to the insurer, including its BoD. The in-depth individual assessment by FINMA of each insurer provides the insurer an external perspective on matters that are instrumental for its safe and successful operation.

C. Purpose of this Report

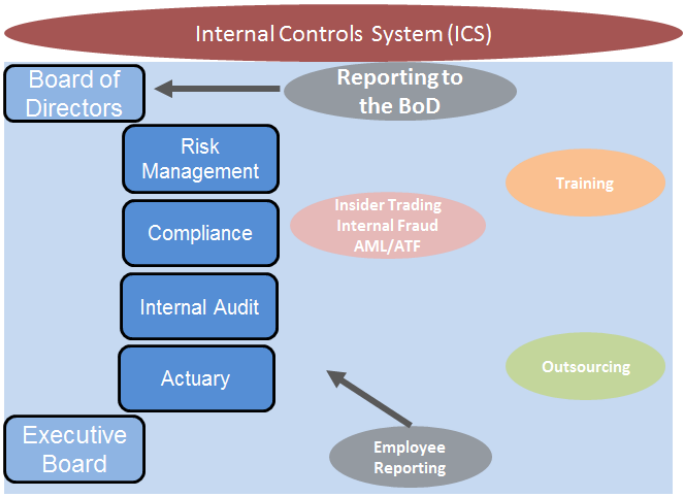
In this report FINMA shares the insights it gained from SQA II from a macro perspective. This includes practice trends and strengths and weaknesses which FINMA observed across the insurers reviewed.

As such, this report should be of comparative value to each insurer (whether or not it was reviewed under SQA II) in its efforts to enhance or calibrate its CG/RM/ICS practices and performance. It should be of particular utility to Boards of Directors in carrying out their duty of oversight in the aforementioned areas.

To further enhance the value for insurers, the report points to relevant differences found in the practices or performance of Groups versus Solo insurers. Life versus non-life differences are also indicated where major differences were observed.

D. Areas Covered by SQA II

FINMA used eleven main modules or indicators[2] in SQA II to gain a more ample and robust view of an insurer's governance, risk and control environments and the corporate culture within which the company operates. The analysis was supported by additional information and insights gained by FINMA through its regular on-going supervision of the insurer. For smaller insurers adaptations to the SQA II scope and depth were made to accommodate the lower risk profile.



E. Overview of Main Observations

The detailed observations are provided in the Appendix. This part summarizes the key observations.

1. *In general, a positive maturation trend is observable among reviewed insurers in many, though not all, CG/RM/ICS areas. Examples of noticeable development in general include:*
   - Better focus on governance structures and processes, both at the BoD level and at the Management level, with improved attention to reducing arrangements where decision-making is unduly concentrated in one person or in a small number of persons.
   - Advances in risk management and internal controls both in the general approach and in the application of specific tools and methodologies.
   - Higher sensitivity at most insurers to compliance risks and, to a lesser degree, to the underlying culture and values of the company.

[2] The indicators are the 1) Board of Directors, 2) Information provided to the BoD, 3) Governance of the Management Board, 4) Risk Management, 5) Internal Controls System, 6) Internal Audit, 7) Actuarial Function, 8) Compliance Function, 9) Compliance-Related Risk Areas (Anti-Money Laundering, Insider Trading, Employee Reporting Mechanisms and Internal Fraud Prevention), 10) Employee Training on Risk and Compliance topics and 11) Outsourcing.

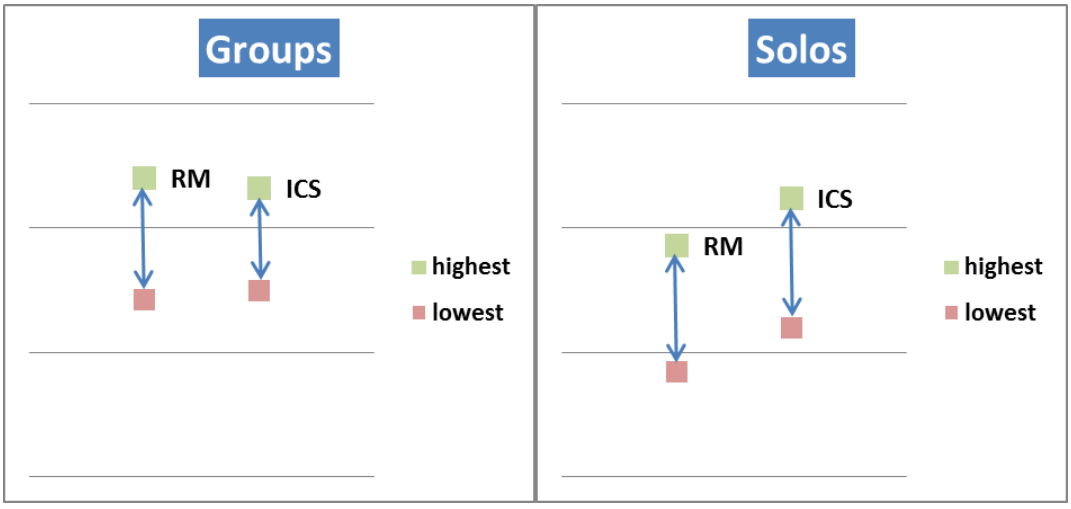
2. *Progress, however, remains uneven across insurers*.

- Groups in general, and particularly the larger Groups, demonstrate higher GC/RM/ICS awareness and efforts in most (but not all) areas than Solos.

> However, Groups also show certain shortcomings in the consistency of their execution, including at the business unit or single entity level. In some cases it is not clear if "Group-wide standards" apply throughout the Group or if the adherence to those standards is sufficiently monitored and enforced by the Group.

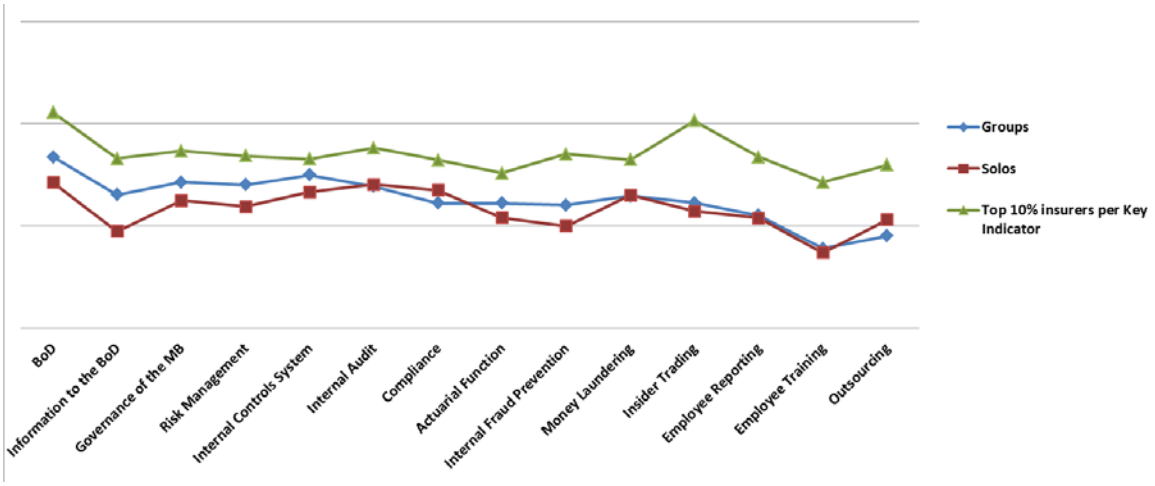
- Moreover there are noticeable differences between Groups with the highest SQA II performance and those with the lowest. This is particularly true in the areas relating to the governance of the Management Board, Risk Management and Compliance.
- The differences are even more pronounced among Solos. For these insurers, there is a wider spread of performance in the CG/RM/ICS areas. This suggests that some Solos—relative to each other—have significant catch-up needs.
- The spread among Solos is smaller as regards the BoD but significantly bigger in respect of Risk Management and the Internal Controls System.

Spread of RM/ICS performance on SQA II between Groups and Solos



- Among health insurers, some show a need for intensifying their efforts in nearly all areas.
- SQA II shows no significant differences between life, non-life and reinsurers in general.

Comparison of performance between Groups and Solos on the Key Indicators of SQA II



3. *There is heightened awareness in general by BoDs of their duty to provide oversight of Management and of risks. But there are questions on a) whether BoD informational needs are always being met and b) BoD time availability.*

- BoD members are giving more thought to risk and are seemingly more willing to engage Management on specific risk issues.
- But there are questions on whether all BoDs are receiving all the information they need to understand the full risk picture of the insurer and make sufficiently informed decisions.
- Also, despite more awareness about 'emerging risks', BoDs appear not to be receiving enough forward-looking information that can give them an earlier insight before risks materialize.

Both BoDs and CROs see better risk reporting to the BoD as the risk area requiring the most improvement.

- In some cases, questions arise regarding the time which BoD members effectively have available to fulfil their duties in light of other mandates.
  - For example, while on average BoD members have 3 mandates, in more than 10% of cases it exceeds 5, and in 5% of cases it exceeds 10.
- Regardless of number of mandates, questions arise in some cases as to whether the time spent by a BoD member is sufficient *from a qualitative perspective* to allow him or her to adequately interact with Management and the Control Functions, digest the information received, determine where additional information is needed, and make well-considered decisions.
- Another area of development for some BoDs relates to their oversight of Control Functions. While in most cases this appears to be adequate in respect of Internal Audit, less consistency and/or intensity is seen with regard to Risk Management and even less to Compliance.

4. *There remain improvement needs in a) the framework and communication of the insurer's risk appetite and specific risk limits, b) risk governance, including the arrangements for the Risk Management Function, and c) the scope and operation of the Internal Controls System.*

- Although there has been noticeable progress, some of the reviewed insurers do not show a sufficiently clear approach in setting their overall risk boundaries or, in some cases, risk limits in specific areas. Sometimes a defined risk appetite statement and risk limits exist, but these are not always communicated amply enough or used as guideposts within the company.
- Some insurers are late in putting in place a dedicated CRO or equivalent or they come up short in demonstrating that such person is positioned so as to be able to a) carry out the full scope of his/her responsibilities and b) provide independent assessment and challenge on risk.

> Some 40% of CROs perceive a need for a higher degree of independence and authority. In some cases the issue is too narrow a mandate. For example, some CROs do not yet have full enterprise-wide accountability.

- There is improvement in insurer approaches to operational risks but, relative to other risk categories, this remains an area with particular improvement potential, especially in terms of risk identification and reporting.
- The scope and operation of the ICS at some insurers remains underdeveloped. Scoping issues arise in terms of covering all needed a) risk areas and/or b) business units/legal entities.

5. *Compliance sensitivity appears to be increasing. But there are remaining shortcomings in (a) structures and execution and (b) effectively addressing certain compliance risks.*

- CEOs are showing greater appreciation for compliance-related topics, also in a cross-border context[3]. Compliance officer access to the CEO is increasing. Codes of conduct are widely in place (a clear improvement since SQA I) and an appreciation of the connection to corporate culture appears to be increasing. Compliance policies in key areas have been developed at most insurers.

> At some insurers, however, there is less evidence of compliance having come sufficiently within the radar of the BoD or of the BoD fully embracing its role in setting the leadership and ethical "tone at the top".

- Progress is not sufficiently rapid at some insurers in developing a Compliance Function with the necessary reach and authority to play a more effective leadership and assurance role. Some insurers have not moved sufficiently beyond the "legal counsel" model such that the compliance officer either lacks the time to focus on compliance strategies and mechanisms or is not suffi-

[3] With regard to cross-border risks, see FINMA Newsletter 37/2012 'Cross-border financial services business – FAQs about the Position Paper on Legal Risks'.

ciently independent and empowered to implement these and effectively drive compliance improvements enterprise-wide.

- In some compliance areas (e.g. conflicts of interest and internal fraud), Solos (but also a few Groups) do not have a sufficiently developed or coherent approach.

  Some 80% of insurers now have in place an employee reporting system (whistleblowing). However, few are taking steps to make enhancements that could give the employee more confidence to report a concern or actual violation without fear of negative personal employment-related repercussions.

6. *There appear to be pervasive weaknesses in (a) the governance and oversight of outsourcing and (b) the training of employees on risk and compliance topics.*

   - Compared to other areas reviewed, the above-mentioned areas received the lowest assessments for the vast majority of reviewed insurers, including Groups.
   - Many insurers using outsourcing (or insourcing within a Group) do not demonstrate having appropriate governance for defining where and how outsourcing decisions are to be made or which reviews (e.g. risk, compliance, etc.) are mandatory. Oversight of outsourcing, including adequate reporting thereof to the BoD and periodic audits, is often insufficiently established.
   - While there is evidence of more training of employees on compliance topics, it is not always pursuant to a defined strategy. This often results in inadequate scope, prioritization or regularity. Training on risk management topics appears minimal.
   - Learning effectiveness of training offered is rarely measured.

7. *Insurers are not sufficiently measuring the effectiveness of their CG/RM/ICS efforts.*

   - Many reviewed insurers lack or are still in an early stage of developing metrics, key performance indicators (KPIs), and other ways to assess the effectiveness of their CG/RM/ICS processes, controls, activities and functions. This impairs the ability of the insurer's BoD, for example, to judge whether the insurer is on the right path. It may also lead to inefficiencies when ineffective measures unwittingly continue to be pursued.
   - Even some Internal Audit Functions lack KPIs or are insufficiently mining the information their audit findings provide. While many track whether their audit findings are implemented by Management, only some perform more advanced analyses of the impact and effectiveness of their audit activities.

   > One emerging good practice at some insurers is to take into account the timely and successful implementation of audit findings in a manager's area of responsibility in assessing that manager's annual performance.

   - The Risk Management, Compliance and Actuarial functions are not being regularly assessed as functions at many insurers.

- The above shortcomings may help explain why some insurers are unsure of the impact of their risk mitigating measures on (a) their company's overall gross risk profile or (b) the gross risk profile in a specific risk category.
- These shortcomings may also help explain why some insurers show less command of their aggregated risk picture or that of individual business areas or units. Not knowing more precisely the relative CG/RM/ICS performance of individual areas or units could result in capital allocation, remuneration and other critical decisions being made which do not accurately reflect such performance and thus the effective risk being taken.

8. *At some insurers there may be an underinvestment in the CG/RM/ICS areas.*

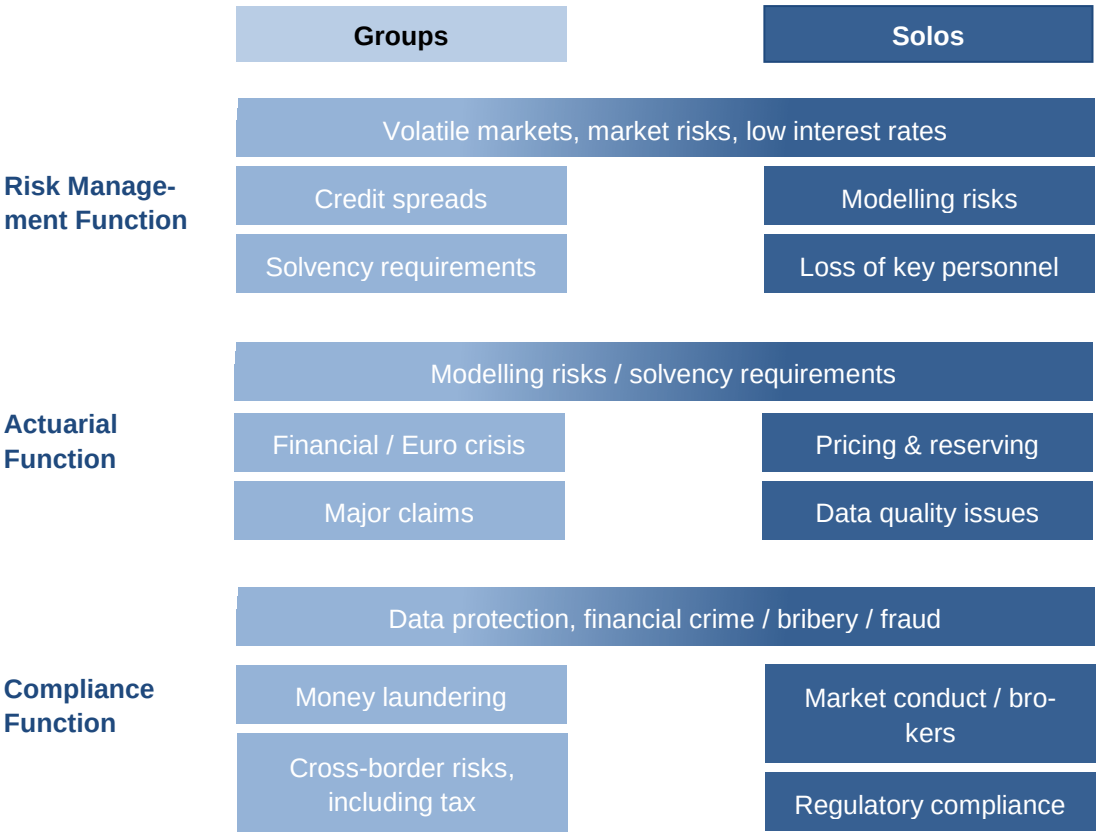
- There are marked differences among insurers of similar size and risk profile in the resources they apply in the CG/RM/ICS areas. This appears to be particularly the case in respect of the Internal Audit Function.
- To the extent that resources appear low at some Solos, it is possible that some of these insurers have not incorporated sufficiently in their business model and financial planning the necessary costs of appropriate CG/RM/ICS activities. This results in severe pressures on the Control Functions to perform without being provided appropriate staff and other resources. Or in some cases it may result in Control Functions reducing their scope or intensity of efforts.

Some insurers are unaware of their internal spending in the CG/RM/ICS areas or have not developed the means to track accurately the various components of such spending. For example, some Solos have no distinct budget for the Compliance or Actuarial functions.

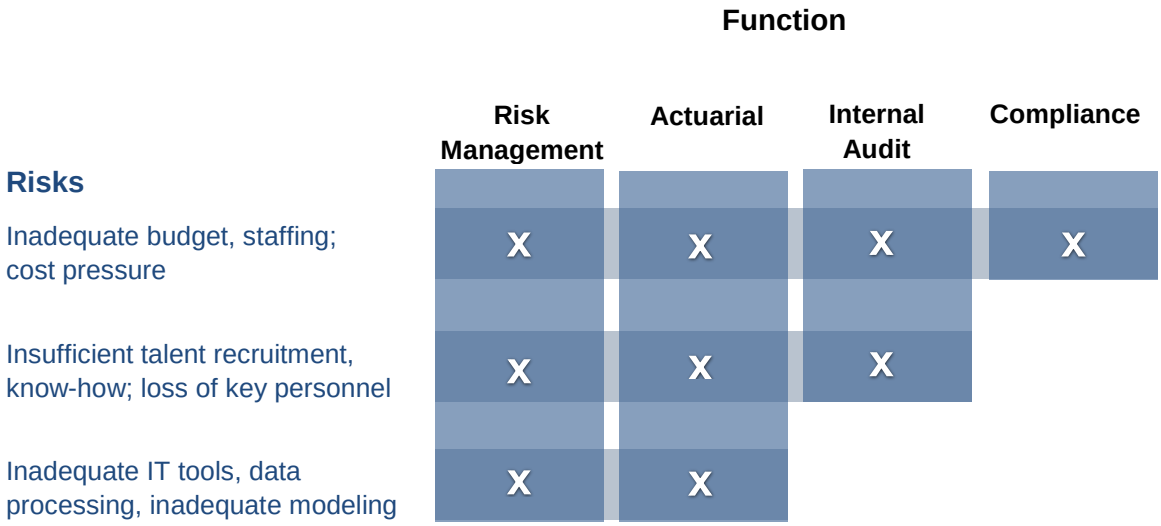
- At some insurers the Control Functions have limited say or influence on the resources they deem necessary to carry out their assigned tasks and responsibilities.
- Information on budgets, resources, and other investments in the CG/RM/ICS appears not always be sufficiently reported to the BoD such that it can provide oversight and approvals where appropriate.

9. *Low interest rates, market financial instability and compliance challenges are top risks facing insurers, as seen by their Control Functions.*

Top risks to the company as perceived by each Control Function:



10. *For Control Functions, the most common risks they believe they face as functions and the areas where they see greatest development need relate primarily to resources, know-how, and IT-related and modelling needs.*



More information and a more detailed analysis of the SQA II observations are provided in Appendix II.

F. Other Observations from SQA II

1. Role of supervision in qualitative areas

FINMA's experience with SQA II points to a growing recognition by Swiss insurers of the need and role of supervision in qualitative areas.

Insurers in general show openness and willingness to engage in the topics covered by SQA II. Some express that FINMA's review has brought new ideas or led to new perspectives on their own internal efforts. Insurer responses generally reflect good consideration of the issues being reviewed. In comparison to SQA I, FINMA senses more willingness by many of those responding to be self-critical where justified, and to point to areas where, in their view, more work at their company is needed.

FINMA's SQA II assessment of an insurer includes specific observations, recommendations, and, where warranted, demands for action.

Both during the SQA II process and following the risk dialogs FINMA was able to observe numerous improvements by insurers in the areas reviewed, some in fundamental aspects of company practice.

2. Multi-level supervisory interaction

SQA II confirms the mutual benefit of supervisory interaction not only with senior management but also with members of the BoD and heads of the Control Functions.

It was valuable for FINMA to obtain directly the views of the BoD Chairs regarding their governance and risk priorities. Similarly, in the exchanges with FINMA, BoD members tended to show keen interest in receiving FINMA's views on the company's potential exposures. Since BoD members also have to form a view of how well their company is performing in the CG/RM/ICS areas, FINMA's perspective appears to have been valued by many as a useful "external view" and "second opinion".

Direct discussions with the heads of the Control Functions was also very fruitful, serving as a way for better mutual understanding of the priorities from both sides.

3. Use of multiple indicators

The use of multiple indicators proved useful for achieving a more comprehensive and robust assessment but also a more balanced one.

The SQA II approach, with the use eleven main indicators, permitted going in depth in specific areas while keeping a view of the "big picture".

The use of multiple indicators also facilitated a better understanding of the interdependencies among the various CG/RM/ICS organs and areas of activity at the insurer, permitting thus a more balanced assessment. For instance, in evaluating an insurer in terms of its outsourcing, FINMA could also note the extent to which any weaknesses in the insurer's general risk assessment processes could adversely affect the risk assessments in outsourcing. Inversely, this approach also allowed FINMA to take appropriate account of the strengths in one area (e.g. the existence of a strong risk committee) as a partial mitigant for a still developing risk management function.

G. Conclusion

1. Mutual benefit

SQA II has provided FINMA a more complete and robust enterprise-wide risk view of an insurer. It has also given FINMA more extensive insights on the Swiss insurance market as a whole. These insights are assisting FINMA in its efforts towards more effective, risk-based and prioritised supervision.

At the same time, input from the reviewed insurers suggests that the SQA II process has been of value to them in better understanding where they stand in relation to the market and in identifying where changes may be needed. In those cases where FINMA's assessment differed with that of the Insurer's

BoD or Management, this has stimulated internal company debate and facilitated a more substance-based dialog with FINMA.

2. Company responsibility

The SQA II assessments are not intended to reduce the need for on-going oversight by the insurer's BoD in the areas in question or to reduce Management's responsibility for quality implementation. They are also not meant to reduce the accountability of the Control Functions in carrying out their independent assurance role.

FINMA expects the BoD of each insurer (whether or not reviewed under SQA II) to continue to satisfy itself regularly—in consultation with Management and the Control Functions—of their company's arrangements and performance in the CG/RM/ICS areas. On the next page are six questions which a BoD may consider in this regard.

1. ***Is the overall governance system of our company still appropriate in light of any recent changes in our size, complexity, risk profile or market best practices and foreseeable changes in the external risk and regulatory environment?***
    - *Is this system operating effectively?*
    - *Do we have the right checks-and-balances at the BoD and Management levels?*
    - *If we are a Group, is this system equally strong at our subsidiaries?*
2. ***Is our BoD properly composed, with the experience and skills to understand the business we are supervising?***
    - *Do we have the right committees and do they work effectively together?*
    - *Do we evaluate our own performance? Do we get sufficient training?*
    - *Are our BoD members devoting sufficient quality time to their duties?*
    - *Are we receiving the right information from Management and the Control Functions to understand our company's risks and make informed decisions about them?*
    - *Are we supervising enough the company's approach to managing risks and complying with laws and regulations?*
3. ***Is the culture of our company conducive to responsible conduct?***
    - *Is the company pursuing the right initiatives in the CG/RM/ICS areas, including sensitizing and training employees?*
    - *Are we exposed to internal fraud, money laundering, insider trading or other integrity risks?*
    - *How sensitive are we to conflicts of interest? Do we have a reliable process to identify and address such conflicts?*
    - *Can our employees report concerns or violations without fear?*
4. ***Do the Control Functions (Risk Management, Internal Audit, Compliance, and Actuary) have the necessary authority, independence and access to information and people to be effective?***
    - *Does their organizational reporting structure help or hinder this?*
    - *Do they have enough resources? The right personnel?*
5. ***Do we review often enough the effectiveness of our company's risk management and internal control systems and of the Control Functions?***
6. ***Do we outsource (or insource within a Group) any critical activity or function?***
    - *If so are these being subjected to at least the same (or where appropriate more) oversight and risk and compliance review as those which have not been outsourced (or insourced)?*
    - *Is the BoD getting appropriate information on the above regularly enough?*

APPENDIX I: Outline of Detailed Observations

1. BOARD OF DIRECTORS

a. Overall: better oversight awareness, some potential blind-spots
b. BoD expertise in general well-balanced; some insurers show gaps
c. Time availability a question mark
d. Resources for the BoD appear adequate
e. BoD practices on its own work show variance
f. BoD interaction with Management and Control Functions rising but not equally

2. INFORMATION RECEIVED BY THE BOARD OF DIRECTORS

a. Overall satisfaction with information received from Management
b. Open questions on the information from the Control Functions

3. MANAGEMENT BOARD

a. Overall: better governance also at the management level
b. Mix of MB models are being used
c. Positive development: increased use of management committees
d. For some insurers there are still major improvement needs

4. RISK MANAGEMENT

a. Overall: general improvements
b. Risk expertise increasing
c. Positioning, authority and independence: improving but not at all insurers
d. Other observations
e. Communicating internally on risks: some good practices but remaining improvement opportunities
f. Gains and gaps in strategy and scope of the RM Function
g. Improvement needs in clarifying the overall risk appetite framework and risk limits; more needed on communication and use
h. More focus on operational risks is taking place but there remains considerable improvement potential
i. Risk Management Functions face risks but are looking ahead

5. INTERNAL CONTROLS SYSTEM (ICS)

a. General forward movement
b. Approaches to managing the ICS vary but some trends are emerging
c. ICS scope and full implementation: a remaining challenge
d. Effectiveness testing is still in an early to mid-stage; documentation of control overrides is weak

6. INTERNAL AUDIT

a. No material deficiencies generally
b. Generally appropriate positioning, authority and independence
c. Questions on resources
d. Some inconsistencies on basic practices
e. There are some development needs for Internal Audit Functions

7. ACTUARIAL FUNCTION

a. More coordination of actuarial activities is taking place at many insurers
b. Inconsistencies on actuarial policies and guidelines
c. Wide differences in actuarial information reporting
d. Management-level committees are being used to buttress the Actuarial Function
e. Challenges remain for the Actuarial Function
f. Assessments of Actuarial Functions still insufficient

8. COMPLIANCE FUNCTION

a. Compliance sensitivity appears to be increasing
b. BoD engagement on compliance less visible
c. Shortcomings remain in compliance structures
d. Progress on compliance policies but compliance strategies still not well developed
e. Greater attention needed on customer-focused compliance and on conflicts of interest
f. Evidence of good practices but also of on-going improvement needs

9. COMPLIANCE-RELATED RISK AREAS

a. Anti-Money Laundering / Anti-Terrorist Financing mechanisms are in place but many remain basic
b. Preventing insider trading: widespread use of policies but scope and preventive measures vary widely
c. Policies for employees to report concerns or violations are increasing but there are insufficient efforts to optimize
d. Internal fraud prevention generally moving on right track but intensified efforts are required

10. EMPLOYEE TRAINING

Compliance and risk training: a strong development need

11. OUTSOURCING

Governance and risk assessments of outsourcing: a potential weakness area

APPENDIX II: Detailed Observations from SQA II

1. BOARD OF DIRECTORS

a. Overall: better oversight awareness, some potential blind-spots

In general, the SQA II assessments suggest heightened awareness by many BoD Chairs and other BoD members of the role of the BoD, as the highest governance organ of the insurer, in providing oversight of:

- Management
- the company's key risks

BoD members, for example, appear more willing to engage Management on specific risk issues, such as in relation to capital and solvency and how risks are weighted. For this the use of specialized BoD committees is more prevalent.

> Three quarters of the BoDs of Groups now have a Risk Committee. The use of Risk Committees appears to be both an effort to allow deeper dives into specific risk issues as well as a way of relieving the workload of the Audit Committee.

Some BoDs are also engaging in more structured planning of the work of each committee or are holding BoD sessions with specific thematic focus. Others are doing periodic reviews to ensure there is a good balance between the work done by committees versus that done by the BoD as a whole and are assessing how the BoD's decision-making process can be optimized.

The most common BoD committees remain the Audit, Risk, and Compensation & Nomination committees.

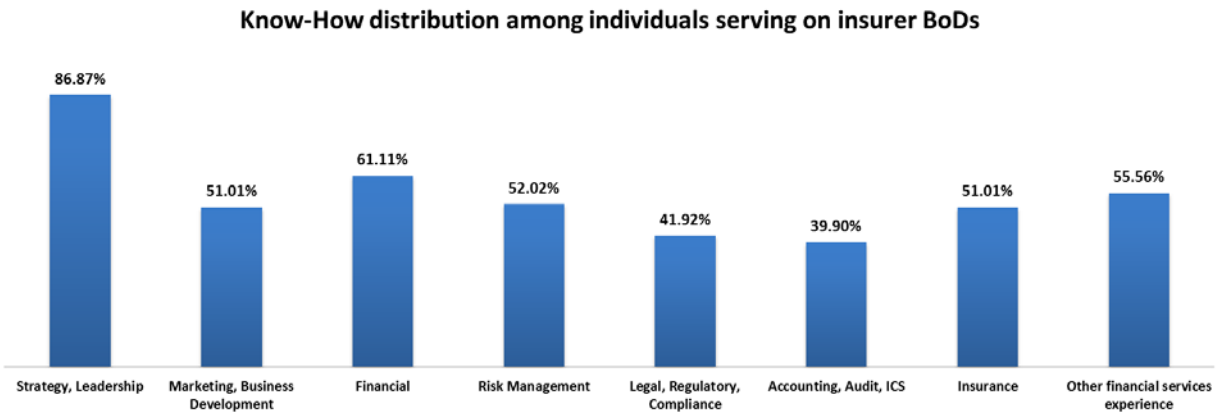
Looking ahead, BoDs may wish to review their existing committees and their mandates to ensure all critical areas are being covered. For example, if an insurer's business model calls for more outsourcing (see Section 11, below), a closer review of that area by a committee may be appropriate. Major risks from IT-security, cyberspace, and data protection are examples of other topics that in some cases could benefit from more regular BoD committee oversight. In some instances, rather than increasing the mandate of an existing committee, a new committee may be in order. Some insurers, for example, have put in place a Governance Committee to deal with the higher expectations in this area.

In general BoD Chairs indicate having the means to obtain a clear view of their company's overall CG/RM/ICS environment. However, for some Chairs this is not the case in all CG/RM/ICS areas.

Together with other indicators, this may suggest that there could be areas at some insurers where a BoD either does not look deeply enough or is not provided the necessary information by Management or the Control Functions. If severe enough this could lead to blind-spots where the BoD is unaware of a risk until it materializes.

b. BoD expertise in general well-balanced; some insurers show gaps

Overall the expertise among BoD members of reviewed insurers shows a healthy spectrum in areas relevant to the oversight of an insurer. This includes broad areas, such as in relation to strategy and financial services, as well as more specific fields such as accounting. It is noteworthy that nearly all insurers now have at least one member with risk specific expertise on their BoDs. While the depth or quality of this expertise is not clear, it is a significant development.



On the other hand, not all insurers have an appropriate distribution of experience and expertise within their BoD. Some have an under-representation, for example, of insurance or financial expertise.

Another challenge for some BoDs is less about having pockets of specific expertise but sufficient diversity of voices and perspectives among its members. Such diversity could assist a BoD in identifying new opportunities and dealing with problems for which multiple views can be helpful.

FINMA is observing various efforts by BoDs to deal with these challenges, such as:

- broadening recruitment efforts and improving succession planning;
- setting additional competence requirements for those BoD members serving on specialized committees and considering this in the general recruitment of BoD members;
- setting term limits as a way to contribute to periodic renewal and rebalancing of the BoD membership with the needed experience or expertise (some 5% of insurers have BoD members who have served for over 15 years).

c. Time availability: a question mark

In some cases, at both Groups and Solos, questions arise regarding the time which some BoD members effectively have available to fulfil their duties in light of other mandates. For example, while on average BoD members have 3 mandates, in more than 10% of cases it exceeds 5, and in 5% of cases it exceeds 10. Examples of individuals having over 20 mandates were also found.

Among BoD Chairs the time devoted to their task at an insurer varies considerably. In 17% of cases this is less than 15 days per year, while in 35% of cases it is over 75 days. On average, the number is 93 days among Groups and 35 days among Solos.

The chart below shows the average days devoted by the BoD Chairs as well as by Chairs of the Audit and Risk Committees of all reviewed insurers.

In general, the Chairs of the Audit and Risk Committees find they have sufficient time at their meetings to discuss in depth and adequately address the matters on their agendas. However, there are some differences. The satisfaction appears higher among the Chairs of Audit Committees of companies also having a Risk Committee. This suggests that having a Risk Committee can relieve potential overload of an Audit Committee and allow it to deal more effectively with its mandate.

In terms of number of meetings by the BoD, a wide range can be observed. For example, some BoDs meet over twelve times a year, while others merely two or three times. Among Groups the average is some 7 times per year.

The key question for some BoDs is not just the number of meetings or the rate of BoD member attendance at such meetings but whether members are fully engaged. This includes having sufficient quality time to a) thoroughly prepare for such meetings, b) adequately interact with Management and the Control Functions, c) digest the information received and request additional information where needed, and d) make well-considered decisions. For committee members the additional time required for exploring in more depth the areas of their mandate is another important factor.

d. Resources for the BoD appear adequate

As BoD members seek to carry out their oversight duties, an important question is whether they have available sufficient administrative and other support, and appropriate IT tools.

BoDs appear generally satisfied on both counts, particularly BoDs of Groups. For example, over 80% of Group BoDs find the BoD budget and staff support available to them to be adequate. However, this

drops to under 70% in terms of the adequacy of the IT tools (such as BoD specific portals). Among Solos the trends are similar, with slightly lower satisfaction with the overall budget available.

With respect to the means to hire external experts when the BoD deems it necessary, the satisfaction remains high but less so than on the above subjects. Some Solos particularly would see an improvement need in this respect.

e. BoD practices on its own work show variance

Satisfaction with dynamics: In general, BoD Chairs find positive the internal BoD dynamics. Over 75% are satisfied or very satisfied in all respects with the interaction and cooperation among its members. BoD culture is often described as “open” and “constructive”. However, some 10% of the BoDs of Solos and 25% of the BoDs of Groups see room for improvement. In some cases this may point to improvement need with regards to the BoD work as a whole, the work within BoD committees, or the work of the BoD committees with the full BoD.

Some BoDs are using pre-clearance for additional mandates: In light of the additional demands that taking on more mandates can make on a BoD member, some BoDs require pre-clearance from the BoD Chair or the full BoD before a member takes on a new mandate. Less clear is how those BoDs that do not have such requirement review a member’s additional mandates for possible conflicts of interest before the member commits to them.

BoD membership showing generally better practices: To allow the BoD to fully exercise its independent duty to supervise Management and to maintain the needed separation between oversight and operation, insurers are showing more diligence in avoiding practices that compromise these goals. The chart below shows some of the best practice configurations in BoD membership identified through SQA II and additional considerations for some of them.

Type of BoD	Type of BoD Member		
	Independent External Members (employed neither by the entity in question nor by any entity that is part of the same Group; otherwise not having any conflicts of interest)	**Group Members** (not employed by the legal entity in question but employed by another entity within the same Group)	**Management Members** (employed by the legal entity in question or delegated by a related entity to serve as a Management member of the legal entity in question)
Group BoD	100% independent external members	None	None
BoD of a Group subsidiary	Use of independent external members, particularly 1) as BoD Chair and/or Chairs of BoD Committees and 2) if it is a significant subsidiary. In some cases, the independent external members are also on the BoD of the Group or another Group legal entity	If used, the individuals are selected carefully to minimize conflicts of interest. <u>Important to:</u> • provide them training on their distinct duties as BoD members. • have mechanisms to deal with any conflicts of interest from these individuals wearing two hats. • do periodic reviews to ensure checks-and-balances are working and the interests of the legal entity are being properly protected.	Use of Management members is avoided in order to preserve checks-and-balances and avoid mixing oversight and operational responsibilities, particularly if it involves the CEO or other leading manager of the entity in question.
BoD of a Solo (entity not part of a Group)	100% independent external members	Not applicable	

Nonetheless, SQA II also reveals other structures which do not support appropriate checks-and-balances or can result in one person or group of persons in effect supervising their own work. This can occur, for example, when members of Management of an entity—while not members of that entity's BoD—are members of the BoD or MB of another entity which exercises effective control over the entity in question.

BoDs should be attentive to any such situations and focus on substance over form in ensuring that the principle of appropriate checks-and-balances[4] is observed.

This applies also in respect of BoD committees. Attention also needs to be given there to avoid, where possible, undue concentration of power, such as when the BoD Chair also serves as Chair of an important BoD committee or where the same person chairs more than one BoD committee. Any use of a "Chairman Committee" or similar should also be carefully scrutinized by the full BoD to ensure it does not result in any negative governance repercussions.

More BoD oversight of subsidiary governance. In addition to the issues of BoD membership as described above, the BoDs of some, but not all, Groups are giving more attention to the overall governance practices in the Group's subsidiaries. Towards this end, some Groups now have a Group-wide governance policy to ensure that the subsidiaries and their boards of directors also follow appropriate governance practices. For the rest of the Groups, this is an area where catch-up work is needed.

BoD training is taking place but in some cases sporadically. Four in five BoDs hold some type of training for their members. This includes in many cases training for new members (induction training) as well as for existing members. However, in some cases training appears to be ad hoc and not based on an analysis of where a knowledge or sensitivity gap may exist or where re-enforcement is needed.

Some training also appears irregular and informal (such as in the form of presentations rather than sessions with specific learning goals). Moreover, in some instances the training appears to be more of a side activity rather than a prioritized goal to increase BoD member skills and effectiveness.

The topics most often covered in BoD training are Code of Conduct, general governance, and financial reporting.

Surprisingly at nearly half of the insurers there has been no recent training on the legal duties of a BoD member or on conflicts of interest.

BoD assessments are increasing. Nearly 60% of BoDs are now conducting some type of assessments of their performance. In some cases this involves a formal assessment of the BoD by an independent third party. At most insurers collective self-assessment by the BoD members is more prevalent, while at other insurers the assessment is led by the BoD Chair.

[4] FINMA Circ. 08-32, in particular margin nos. 5, 10, 11.

Less frequent are evaluations of BoD committees and of individual members of the BoD. However, some insurers are doing such evaluations, also evaluating the Chair of the BoD and the Chairs of the BoD committees.

Assessments of the BoD's own documentation—for example in respect of updating its organizational rules and charters where needed and improving how its meetings are minuted—shows mixed results, with some BoDs not undertaking such efforts on a regular basis.

BoD remuneration predominantly in form of fixed honorarium. SQA II did not review remuneration within an insurer. However, it did gather limited information that suggests that very few BoD members are being remunerated in their capacity as BoD members through variable pay, properly avoiding thus the issues that can accompany bonuses.

More attention to succession planning. The BoDs of various insurers are giving this area priority focus in terms of the BoD itself but also of Management. As part of their oversight of Management, these BoDs are seeking a better understanding of the risk of loss of key managers and the contingency preparations that are in place in case of expected or unexpected departures.

f. BoD Interaction with Management and Control Functions rising but not equally

The ability of a BoD to fully understand the insurer depends in part on the information with which it is provided (see 'Information to the BoD' in Section 2 below). But it also depends on the insights the BoD gleams directly from interacting with a variety of senior managers (including but not only the CEO) and others at the company.

BoDs are pursuing various practices toward this end. These include:

- having MB members, besides the CEO, also attend BoD meetings, even when they are not presenting
- holding off-site events with MB members
- interacting with members of Management and of the Control Functions through bilateral and other meetings outside the regular BoD meetings and events
- having meetings with the heads of Control Functions without the presence of Management
- attending employee events to get a better sense of the corporate atmosphere.

A number of BoDs have set as part of their future priorities improving interaction with senior managers and improving the BoD's ability to assess the quality of senior Management members.

Some BoDs are also ensuring that the pursuit of increased interaction with Management is not such as to prevent the BoD from being able to deliberate on its own. Thus, some BoDs reserve part of each meeting for a session with no Management presence.

With respect to BoD interaction with Control Functions, the highest level of interaction appears to be with the Internal Auditor, at least on the part of the Audit Committee. Interaction with the CRO appears to be increasing but is still limited at some insurers. Comparatively less interaction appears to be taking place with the Compliance Function and the Actuarial Function.

2. INFORMATION RECEIVED BY THE BOARD OF DIRECTORS

a. Overall satisfaction with information received from Management

The BoDs of most insurers indicate general satisfaction with the quality and timeliness of the information they are receiving from Management. However, for only a small minority of the BoDs does such information surpass regularly their expectations.

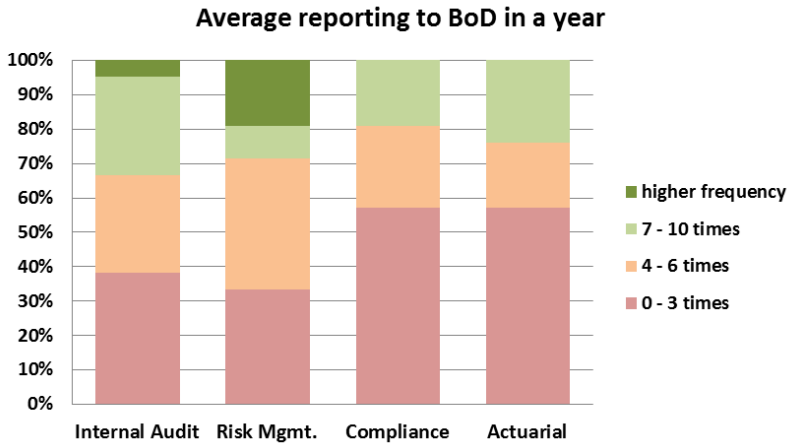
BoDs generally view information provided by Management as useful for their understanding of the risks that accompany business opportunities. This is a positive indication of more Management focus on both the upside and downside of proposed business initiatives and transactions. However, satisfaction in this regard is lower among the BoDs of Solos than those of Groups.

Since a BoD has to understand not only the total performance of the Group but also of its major individual business units and lines, it is also positive that most BoDs find that Management is providing them with the information necessary for this purpose. However, satisfaction appears higher in terms of understanding the financial performance of such units or lines than in understanding their performance in the areas of risk management, controls and compliance. This correlates with other improvement needs which SQA II found in these areas (see Sections 4, 5, and 8 below).

b. Open questions on the information from the Control Functions

As shown in the subsequent sections of this report, there are considerable differences among insurers in the stage of development of their Control Functions. This has an impact on these functions' ability to be of value to the BoD, for instance in terms of providing timely information and independent assessments of the insurer's risks.

One important factor is how regularly these functions report to the BoD. In general, the reporting appears adequate for the Internal Audit Function (on average over 5 times a year for Groups and 4 times for Solos). For Risk Management Functions, while the trend is increasing, shortcomings still exist. In some instances the reporting to the BoD is only once or twice a year, hardly allowing for the type of regular active dialog between the BoD and the CRO that is necessary to deal with risk issues effectively.



The situation is even less developed with respect to the Compliance Officer and the Actuary. While at some insurers, the Compliance Officer reports to the BoD as many as 7 times per year, at others this takes place only once yearly. Reporting by the Actuarial Function to the BoD is even less regular and at some insurers non-existent.

Despite these shortcomings, BoDs which receive reporting from the Control Functions appear generally satisfied with the information provided, particularly the BoDs of Groups.

However, as discussed later, there are questions on whether

- At a sufficient number of insurers the BoD is evaluating often enough the nature, frequency, and quality of reporting it receives from the Control Functions and assessing where improvements could be made, particularly in terms of making such reporting more useful for the BoD's decision-making.
- The reporting obstacles some Control Functions face are adversely affecting their ability to provide independent findings and assessments. For example, in some cases not the head of these functions but their manager reports to the BoD, or the reports to the BoD require Management pre-approval.

Other observations regarding the information which BoDs are receiving:

- Both BoD Chairs and CROs see better risk reporting to the BoD as the risk area requiring the most improvement. For example, despite more awareness about 'emerging risks', BoDs appear not to be receiving enough forward-looking information that can give them an early insight before risks materialize.

BoDs and CROs may wish to work closer together to agree periodically on the type of forward-looking indicators that would be most useful to the insurer.

- Regular reporting by a Control Function can also help the BoD provide oversight of such a function. If the reporting from the CRO, for instance, is regular this can assist the BoD in judging the CRO's effectiveness and better understand the Risk Management Function and its strengths and improvement needs. The BoD's views are critical for ensuring the Control Functions are and remain fit for their duties.
- Some BoDs are also receiving periodic reporting from other functions involved in controls, such as the Internal Controls Manager or the Financial Controller.

3. MANAGEMENT BOARD

a. Overall: better governance also at the management level

A well-structured and run management board (MB) or similar is instrumental not only to better manage the company but also to avoid any undue concentration of managerial decision-making in one person.

SQA II reveals progress also in this area. Insurers are achieving greater clarity by defining and documenting in the organizational rules or similar the role of the MB. This includes setting out its mandate, how it operates (frequency of meetings, etc.), and how it makes decisions. These efforts are also helping insurers address the fundamental issue of whether the MB is a voting or merely consultative body, what powers are exclusive to the CEO, and what checks there are on the these powers.

Better governance of the MB is also helpful in bringing clarity to the boundaries between the BoD and Management. It also assists the BoD in carrying out its supervision of Management by providing a framework it can monitor, with better transparency of how Management operates and arrives at decisions.

b. Mix of MB models are being used

Insurers continue to operate with a mix of MB models. Some larger as well as some smaller insurers are still using the model of a MB that is consultative to the CEO. In such cases all final managerial decisions rest with the CEO, though he or she may gather the various views of the MB members or even try to find consensus before acting. Other insurers have moved to a model where all MB members have a vote.

Slightly more than half of the Groups are now using the voting model, with differences on the extent to which the CEO has a tie-breaking vote, a double vote, or outright veto power. In some cases even where the CEO is authorized to overrule the majority of the MB, the organizational rules require that the CEO report any instance of such override to the BoD Chair. At some insurers with voting MBs there are still some decisions (e.g. for certain type of hiring) which are subject to the sole discretion of the CEO.

c. Positive development: increased use of management committees

SQA II suggests that there is more use of management-level committees at insurers. These are sometimes committees of the MB or are otherwise separate management committees that focus on specific subjects[5].

The use of such committees can increase managerial effectiveness and efficiency by allowing for deeper focus on specific subjects of high importance (e.g. asset-liability management). An additional benefit is that – particularly when representatives of the Control Functions are also included – the committee can add to the checks-and-balances at the insurer.

A sensible, well-grounded recommendation by a management-level Risk Committee, for example, is more difficult to ignore by a CEO or MB than one coming from a single person.

d. For some insurers there are still major improvement needs

The positive developments outlined above are not equally spread among all insurers. Some insurers are working with management models that lack sufficient structure or documentation. At some insurers the structures and documentation are adequate but not the operational processes. For example, at some insurers the MB meets several times a month or even weekly. At others it is only a handful of times a year. At many insurers, Control Functions do periodic reporting to the MB or attend certain MB meetings, while at others this is not the case.

Some insurers have documented structures but appear not to have reviewed them in recent years to determine if they could be optimized both as a managerial and governance matter. The question of whether the CEO should have sole authority in selecting or remunerating MB members (or whether the BoD should have a role therein) is one type of issue that a periodic review of existing arrangements can help resolve.

4. RISK MANAGEMENT

a. Overall: general improvements

In general, SQA II reveals increased improvements – from modest to significant – on risk management at most reviewed insurers. In addition to better overall risk awareness, there is evidence of more focus on specific risk processes and tools:

- more access to the BoD by CROs
- noticeable upgrading of written policies

[5] For example committees for Investments, Asset- Liability Management, Reserving, Reinsurance, Underwriting, Products and Limits, etc.

- increased consistency in risk definitions and classifications enterprise-wide
- better defined processes for risk assessment and monitoring
- more use of scenario planning and other advanced approaches

One example of noticeable progress is in confronting the challenge of emerging risks. Most insurers are now taking initiatives to identify and track such risks, particularly Groups (over three quarters) but also Solos (over half). This is usually done through a dedicated committee which uses both internal and external data for this purpose. While the sophistication of the methodologies employed varies, it is a positive sign that more insurers are working to anticipate potential new risks.

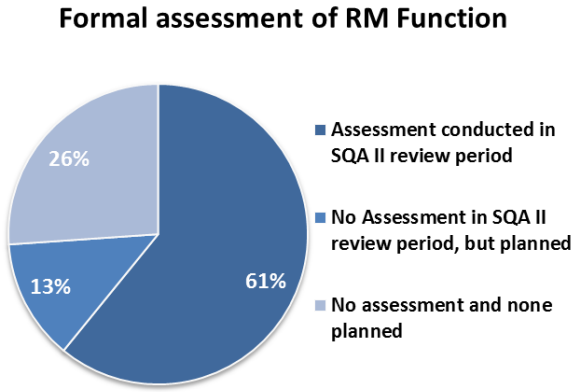
But two factors may undermine these good efforts:

- Not all companies are engaging a sufficiently broad spectrum of people in the emerging risks initiatives (e.g. risk engineers, underwriters, compliance, regulatory, and other experts, etc.). Without these different perspectives the value of these initiatives is reduced.
- It is not clear whether the output of an emerging risk identification process is sufficiently flowing into strategy planning, product design, capital reserving and other processes at the insurer.

Despite the above advances and others described below, most insurers may need to do more to:

- reach or maintain the type of risk management framework and culture that does not leave the company unprepared for known risks or for risks that the company should have reasonably anticipated
- make more timely adjustments and enhancements—before risks materialize—in light of changes in the company's business strategy and market conditions.

To stay up to date insurers are well-advised to frequently review their risk management approach and processes and undergo periodic assessments internally or by an external third party. In this regard, SQA II shows that over 70% of insurers have already had such an assessment or have one planned.



b. Risk expertise increasing

In general, SQA II shows increased risk management specific training and experience by those heading an insurer's risk function.

For example, numerous CROs now have over 10 years direct risk management experience. The average is approximately 7 years.

While RM expertise appears to be growing at most insurers, some insurers are trailing behind. This is more pronounced among Solos but shortcomings also arise within some Groups.

- Within Groups, the gaps are more often at the local entity or country level where risk management functions sometimes do not fully possess the level of RM know-how or risk leadership necessary for addressing local risk needs and/or effectively implementing the Group risk standards.
- In some cases the gaps are on the quantitative side (limited expertise in quantifying risks, modelling, etc.). In other cases the weaknesses lie more on the qualitative side (risk governance, risk culture, assessing non-financial implications of risks and correlating financial and non-financial risks, etc.).

Insurers would benefit from reviewing their current risk skills inventory and, where needed, reenforcing their staff with individuals with deeper or more expansive risk experience or with stronger risk leadership and managerial experience.

c. Positioning, authority and independence: improving but not at all insurers

Even if well-qualified and competent, a CRO may be unable to be effective without the right positioning, authority and independence.

The SQA II assessments suggest growing improvement in this regard. Some companies are already following international best practices in having a CRO who reports directly to the CEO and has unrestricted access to the BoD.

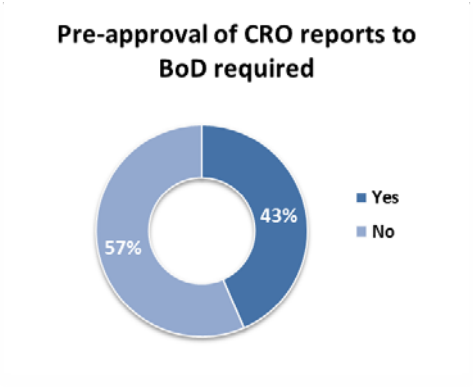
At the same time, significant organizational and reporting hurdles remain for the CRO at some insurers. These include among others:

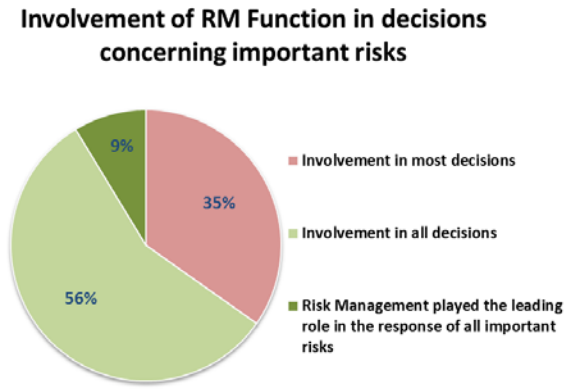
- Not being sufficiently high in the executive hierarchy or having to go through one or more intermediaries to access the BoD. Some CROs do not present all their own reports to the BoD but some are presented by their manager.
- Not having defined written authorities such as to when the CRO has to be informed or consulted or on which matters he or she has to sign off. Some 40% of CROs do not have their authorities sufficiently documented.
- Being given additional and in some cases incompatible tasks such that the CRO may lack the time to fully exercise his/her function or may face potential conflicts of interest.

d. Other observations

- In about half of the assessed insurers, **the documented authority of the CRO does not correspond enough with his/her assigned tasks**. For example, a CRO may be expected to achieve certain risk control goals but his or her written authority may be insufficient to support this. This could lead to unfulfilled expectations and create risk gaps. No major difference here was found as between Groups and Solos.
- In about one third of insurers, the CRO has limited ability to influence the whole of the budget and resources for the risk management function.

- In over 40% of insurers, a **pre-approval of the CRO's reports to the BoD** is exercised by Management. Even if in such cases there are few or no material changes requested by Management, the practice may have a chilling effect on CRO independence and willingness to challenge.
- At half of the insurers, the risk management function is not sufficiently involved in reviewing **risks of new products or material changes in existing products.**
- In about one third of insurers (mainly at Solos), the **Risk Management Function is not always involved in decisions concerning material/important risks**. Interestingly this observation correlates highly to insurers having other weaknesses in the Risk Management Function. This would suggest a vicious circle where a weak Risk Management Function is not called upon to help deal with important company risks, which in fact makes the function even weaker and less relevant.





While FINMA takes no position on the administrative reporting (e.g. who approves expense reports, vacation requests etc.) of the CRO, FINMA is concerned with any impaired functional or substantive reporting of the CRO (on risk strategy, risks, risk assessment, risk reporting, risk policy violations etc.) and with the question of who evaluates the CRO's performance and determines bonuses, salary increases, employment termination, etc. FINMA is also concerned with whether the CRO has access to all the information and people necessary to identify, assess and address risks. These are all factors which can influence the independence and effectiveness of the CRO. BoDs thus should concern themselves with these issues and ensure the practices at their companies are helping to optimize the CRO's ability to provide robust and independent risk assurance. This includes ensuring the company's authority grid indicates those matters on which the CRO's input or sign-off is necessary.

e. Communicating internally on risks: some good practices but remaining improvement opportunities

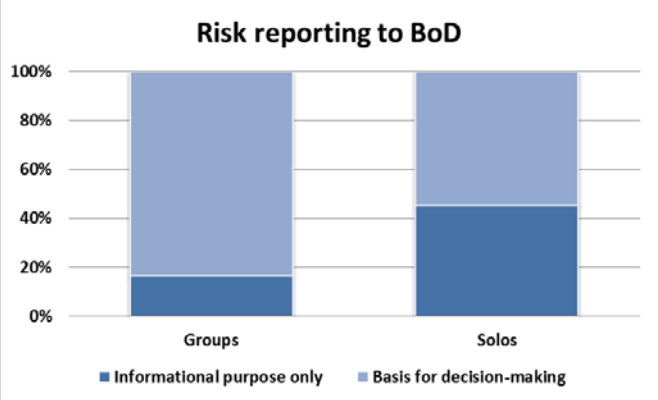
The ability to react promptly on material risks depends in large part on the effectiveness of the reporting and other communication efforts on risk within the company. With changing market conditions and the regular emergence of new risks, this is even more important today.

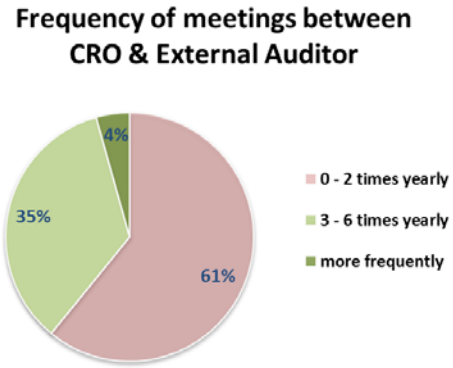
In general, communications between Management and the RM Function appear adequate at those insurers where the CRO is well-positioned. This is also the case at those insurers which have in place a risk committee at the Management level. While such a risk committee does not replace the need for a CRO or for a risk committee at the BoD level, it supplements the risk infrastructure. Also, since the CRO is normally part of such management-level risk committee or chairs, it can help those CROs who do not report directly to the BoD or the CEO.

About two thirds of CROs are able to attend BoD meetings even when not personally presenting a topic. This provides the CRO the opportunity to better understand the strategic and other major challenges facing the company, and raise relevant risk observations.

On the other hand SQA II also reveals improvement opportunities:

- **The formal reporting by the CRO to the BoD varies greatly among insurers in frequency and purpose**. The frequency ranges from monthly up to once a year. Too low a frequency raises questions on the extent of the timeliness and effectiveness of such reporting. In addition at over 40% of Solos and 15% of Groups the risk reports are only for informational purposes rather than for assisting the BoD with decision-making.
- Besides risk reporting, other information-related areas which CROs find need improvement is the **expansion and better use of risk data bases**.
- **The External Auditor is not used enough as an important source of risk-related information.** Only some 40% of CROs meet more than 3 times a year with the External Auditor, while some do not meet at all.





f. Gains and gaps in strategy and scope of the RM Function

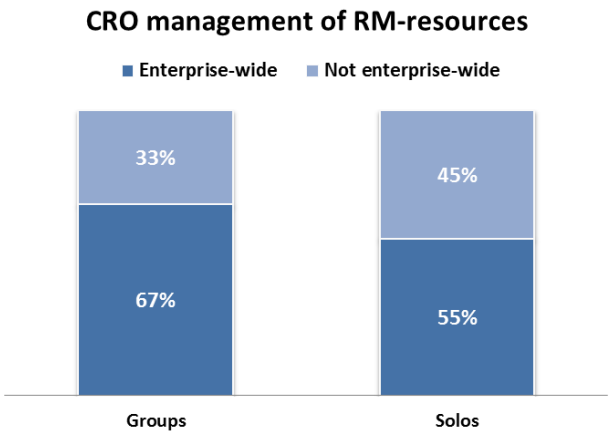
RM Function strategy more prevalent. A well-articulated and documented strategy for the RM Function is a critical instrument for guiding the insurer's risk activities. Four out of five insurers have now formulated such a strategy. The remaining 20% are mainly Solos. However, among insurers where the RM Function has a strategy, only half of these have had it approved by the BoD.

The absence of a sufficiently developed or approved strategy for the RM Function can adversely impact very practical operational decisions. Thus, at some insurers there is little evidence that the RM Function budget is being developed taking into account the function's strategy and the specific risks of the insurer. This could lead to a RM budget which is not tailored to support strategic goals or which is insufficient to permit the RM function to deliver critical services.

Limited Scope. At some insurers it is not clear whether by strategy or default the scope of the RM Function is restricted. The mandate of one third of RM functions does not include all important risk categories. For example, strategic risk—though primarily a responsibility of the BoD and the MB—is not within scope of some 15% of RM functions. Similarly, only 60% of RM functions are involved in overseeing liquidity risk.

Better enterprise-wide reach. There is evidence of more insurers providing the CRO authority to manage risk processes and resources enterprise-wide. This helps the CRO optimize the deployment of risk resources where the greatest risk needs exist. Additionally, it can help increase the independence of individual risk managers through their reporting to the CRO rather than to local business managers. Further, it can increase the ability of the CRO to gain and maintain a full enterprise-wide view of the insurer's risks and better aggregate and correlate such risks.

Among Groups, two thirds of the CROs now have enterprise-wide management responsibility for risk resources. Among Solos which have a CRO, about half of them have enterprise-wide responsibility



g. Improvement needs in clarifying the overall risk appetite framework and risk limits; more needed on communication and use

Apart from meeting the obligations under the SST (primarily the quantitative requirements), many of the reviewed insurers are making additional efforts to define and make clear the quantitative and qualitative risk boundaries within which their company aims to operate.

The starting point for these efforts is typically a frank discussion between the BoD, the CEO, the CFO, the CRO and other key managers on the amount of overall risk the insurer is willing to assume—after meeting the regulatory capital requirements—in order to achieve its defined business goals. Such discussions take into account all relevant factors, external and internal, including the insurer's solvency and liquidity positions as well as its operational capabilities (such as whether the insurer has the risk management resources needed to ensure it stays at all times within the agreed risk boundaries).

Such discussions result in concrete quantitative statements and/or qualitative statements (such as expressing where the company wants to be on the spectrum of conservative to aggressive risk taking). A general company or group-wide risk appetite/risk tolerance statement is then usually accompanied by defined risk limits by line-of-business and by specific activities, such as investments. It could also include prescriptions on risks that the company is not willing to take (e.g. certain geographic risks).

However, not all insurers have advanced as far in this area. For example, some:

- do not have a clear risk appetite framework or, if they do, it is not based a on sufficiently rigorous approach
- are not involving sufficiently the BoD or its Risk Committee in developing and approving such framework
- are not setting clear enough risk limits in specific areas
- are not reviewing regularly enough their risk appetite framework and the risk limits

While a well-considered risk appetite approach and risk limits are essential, they are of limited use if not properly communicated. At some insurers, there appears to be insufficient communication in this regard. For example, it is not clear if all relevant employees know if the company has set a risk appetite / risk tolerance and what it is or, at least, what important risk limits stem from it.

Further, the practical use of agreed limits is not always enhanced. Some companies do not include them in the operational IT systems such as to have a timely early warning system for any breaches of limits.

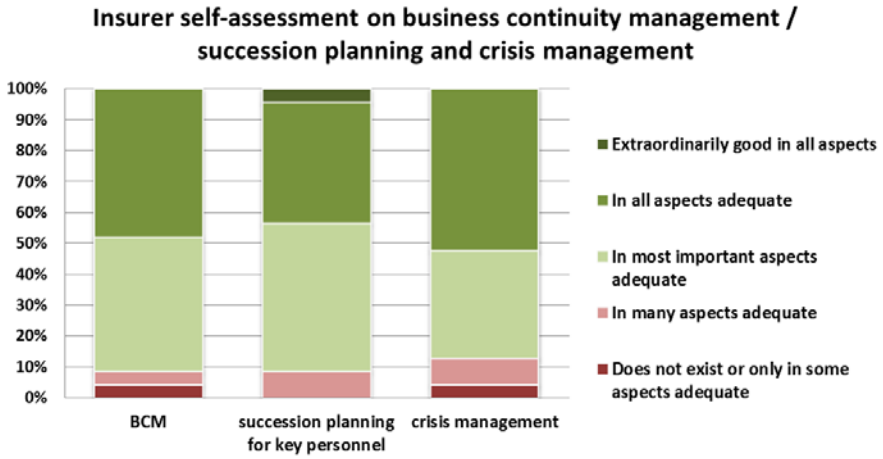
h. More focus on operational risks is taking place but there remains considerable improvement potential

There is evidence of greater awareness among many insurers of the need to pursue a more pro-active and systematic approach to operational risk. This may be due to the growing complexity of operational risks (e.g. relating to IT) and higher corporate sensitivity to the reputational and other impact of operational risk failures (see also observations under Compliance in Section 8 below). For Swiss insurers active in the EU, the quantitative and other expectations of Solvency II have also served as an impetus for more focus in this area.[6]

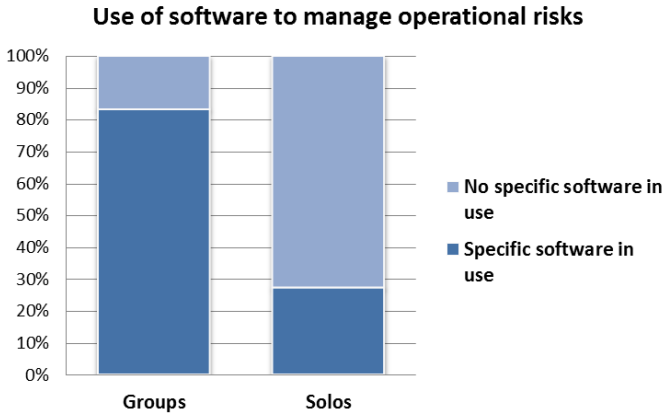
There is in general a more disciplined approach to operational risk as a distinct risk category. Many insurers are now:

- using a combination of top-down and bottom-up means to identify operational risks
- employing scenario-based assessments and simulations
- creating standardized risk registers
- improving tracking and reporting on operational risks
- showing better preparedness on business continuity, succession planning, and crisis management (though for some 50% of insurers there is still considerable work to be done in these areas and there is a small minority that has no plans yet in place)

[6] While FINMA normally does not require quantification of operational risks for SST capital purposes, it does expect their successful management. Further, under Article 98 of the Insurance Supervision Ordinance it is expected that the insurer will capture and assess operational risks. If these results could put solvency at risk, FINMA can intensify its supervision of operational risks and/or increase the required SST target capital. It should be emphasized that it would not be sufficient for an insurer to reserve additional capital without remedying material sources of operational risk.

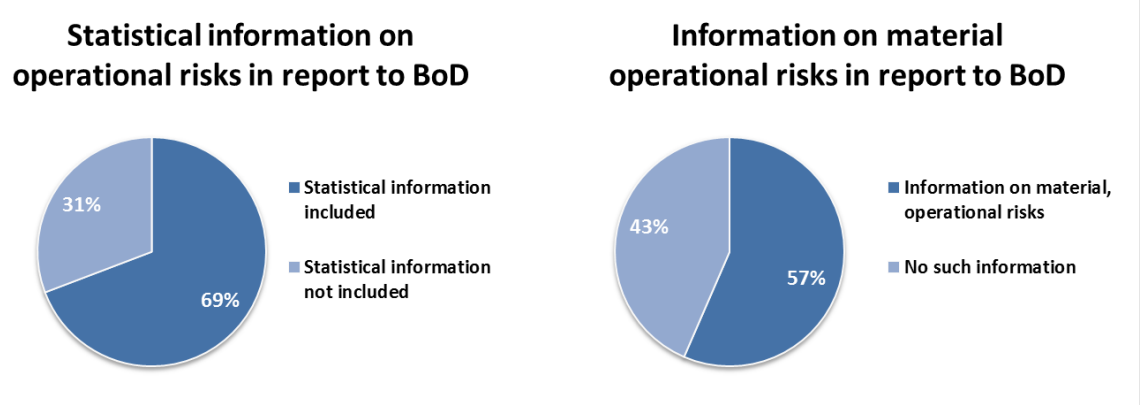


Groups (over 80%) are also making more use of software to help manage operational risks. Among Solos this is only some 20% but the trend appears to be growing.



The use of models and scenarios for operational risks is increasing (particularly among those insurers that are quantifying operational risks) but shows also a lot of variance. In this regard it is not clear how much insurers are supplementing internal loss data with external loss data obtained from outside providers.

With respect to reporting, nearly 70% of insurers now report statistical information on operational risks to the BoD. On the other hand, some insurers do not appear to report all their material operational risk incidents to the BoD. Further, the frequency and quality of reported information varies considerably. For example, it is unclear if the reporting includes a) more forward-looking information and statistics on trends and factors that may affect future operational risks and b) information on the company's performance in managing operational risks.



As the risk management field moves towards more standardized approaches, the pressure to improve the means (methodologies, people, IT) for managing operational risk will increase. SQA II suggests that some insurers are well on their way in this regard, while others are still at an initial phase. All insurers will need to ensure they are not leaving any important risk classes relevant to their business out of their operational risk approach. Some insurers appear to be excluding from their operational risk efforts, for example, reputational, legal, compliance or external claims fraud risks.

i. Risk Management Functions face risks but are looking ahead

The vast majority of insurers (over 90% of Groups and Solos) have identified important objectives and development goals for their RM function. The most common include:

- closer alignment to the business
- more involvement in strategic decisions
- increased efficiency through the use of IT and automation
- more preventive measures

These important goals face some hurdles. Frequent risks which CROs indicate exist for their functions' ability to achieve their goals are:

- insufficient resources (while no CRO foresees a reduction in budget or personnel, 70% of CROs do not expect any major rise despite increasing risk challenges)
- insufficiently sustainable integration of the risk management processes in the company
- weaknesses in risk culture
- insufficient risk data or quality gaps; risk of erroneous reporting

5. INTERNAL CONTROLS SYSTEM (ICS)

a. General forward movement

Among other things, controls serve to ensure that agreed upon policies and processes are being observed and are effective.

As in the case of risk management, advances among reviewed insurers can be seen in their approach and activities on internal controls. This is particularly the case among Groups. At the same time, and similar to risk management, there is a wide spread between the insurers at the higher and those at the lower end of the spectrum regarding the ICS.

Most reviewed insurers are now following one of the internationally accepted standard ICS approaches (with 75% using the COSO framework). Further, the vast majority of insurers now have a central database where key processes and controls are documented and an increasing number of insurers are acquiring or already have in use specialized software for managing the ICS. Less clear is whether the updating is sufficiently frequent (e.g. at a minimum annually).

These efforts reflect a growing recognition of the need to approach controls:

- not as isolated individual controls but as a system or framework that has to be managed and optimized enterprise-wide
- as distinct from other activities, such as policy setting or risk assessment.

b. Approaches to managing the ICS vary but some trends are emerging

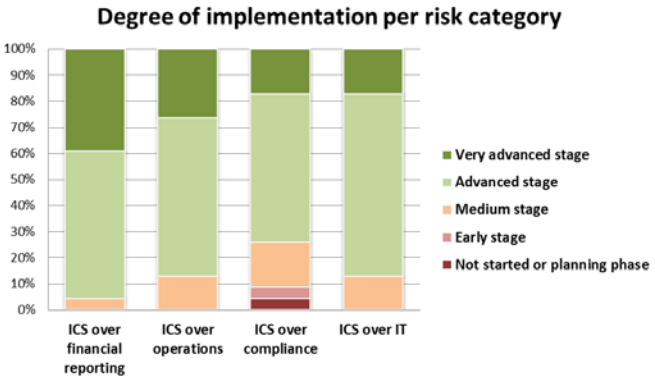
A growing number of insurers are designating an ICS manager or similar to oversee the ICS area. Depending on the size of the company this may be a single person or a distinct unit. At other companies, there is a cross-departmental team or a team anchored in a specific department, typically but not always the Risk Management department. At over 50% of companies, the ICS manager reports to the CRO, but some companies are also working to increase ICS independence by having its head report to the Chief Administrative Officer, Chief Operating Officer, or similar.

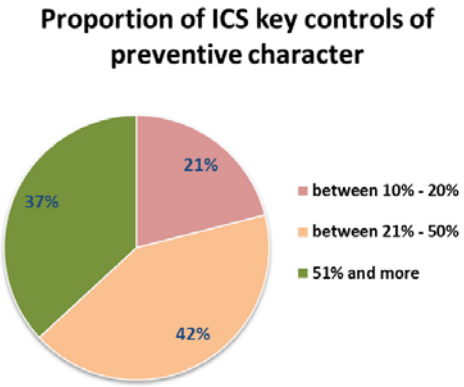
While FINMA does not prescribe the organizational arrangements for managing the ICS, it does look for clarity on how internal controls as a system are managed within the company. It also wants to ensure that, regardless of the arrangement, there is clear focus from a controls perspective and appropriate separation from activities that may compromise the ICS' objectivity.

c. ICS Scope and full implementation: a remaining challenge

Progress among insurers in sufficiently enlarging the scope of their ICS and implementing the ICS varies.

- Not all entities or business units are within the ICS Scope. In 60% of Groups and 25% of Solos, there are legal entities or business units not covered by the ICS. In some cases this is due to insufficient ICS personnel, while in others to a conscious risk choice by the insurer.
- Certain relevant risk types are being left out of the ICS. A few insurers have not brought sufficiently within scope all essential risk types such as in respect of financial reporting, compliance with laws and regulations and key business processes, including IT[7].
- Extent of implementation of the ICS varies. Even when having defined an appropriate ICS scope, some insurers do not demonstrate sufficient evidence of documenting and implementing the ICS in all areas within scope.
- Need for more preventive controls. Approximately one third of the insurers have a proportion of 51% or more of key controls which are of preventive character, while about one out of five insurers have a proportion of 20% or less. A low percentage of preventive controls can adversely affect the overall effectiveness of the ICS.



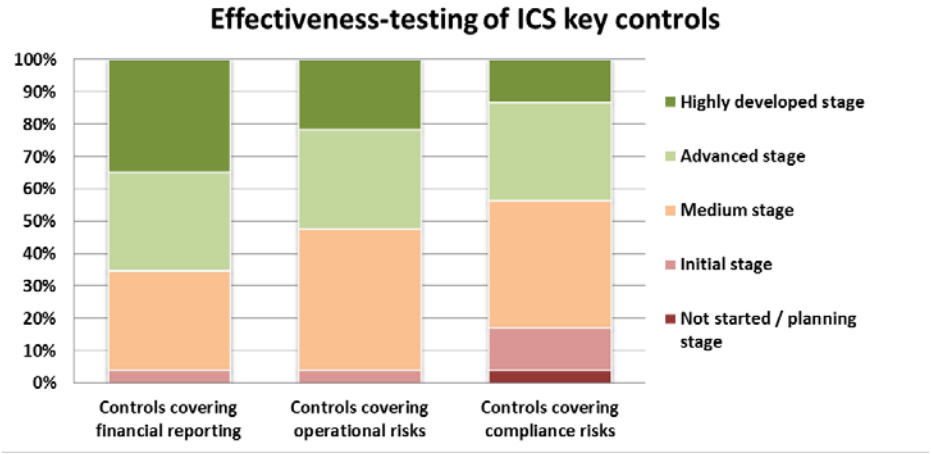


[7] FINMA Circ. 08-32 sets forth that these areas are to be covered by the ICS. This is expected whether or not these areas are being managed in specific departments. For instance, it would not be consistent with the Circular to fail to cover IT risks under the ICS on the grounds that IT risks are being dealt with by the IT Department.

d. Effectiveness testing is still in an early to mid-stage; documentation of control overrides is weak

The testing of the effectiveness of the key controls is developing but at many insurers is still in an early to medium maturity level.

Approximately two third of the insurers deem themselves to be at an advanced or highly developed stage in respect of testing financial key controls. This drops to about 55% for compliance-related key controls. There are also differences among insurers with regard to which functions are involved in the testing. While many use an independent party (e.g. the ICS Manager, Internal Audit, an external party), others rely only on Management, which is insufficient.



The integrity of controls is, among other things, protected by having a process for documenting any overrides of a control by Management. While insurers report that no such material overrides took place during the SQA II review period, only some 60% could demonstrate having a documented process for this. The reporting to the BoD of any material Management control overrides constitutes a good practice and something which BoDs which don't yet require it should consider.

A properly designed and operated ICS supports an insurer's overall risk management efforts. While for some insurers sufficient scoping and initial implementation is an incomplete task, others are more advanced. For these the focus should now be on testing for quality and effectiveness. The reliability of such testing is increased if done by more objective parties. The BoD should periodically satisfy itself of the company's progress in all these areas.

6. INTERNAL AUDIT

a. No material deficiencies generally

SQA II does not reveal material deficiencies in the Internal Audit Function of the vast majority of insurers. In general, internal auditors are the best established of the Control Functions at an insurer. Nonetheless, a number of observed issues suggest a need for action by some insurers.

b. Generally appropriate positioning, authority, and independence

In the vast majority of insurers the positioning of the Internal Auditor is in line with accepted practices whereby the functional reporting is directly to the BoD (usually to the Chair of the Audit Committee). In some cases, FINMA observes leading practices in use, for example:

- To avoid any appearance of interference by Management, 30% of insurers go further in having the Internal Auditor report both functionally and administratively[8] to the BoD.
- At some insurers the BoD follows the practice of having the Internal Auditor attend all BoD meetings, not just those where he or she is presenting.

In only a handful of cases did FINMA observe fully inappropriate practices, such as where the reports of the Internal Auditor to the BoD are not presented by the Internal Auditor but by a member of Management.

One result of the right positioning of Internal Audit is that nearly all Internal Audit heads believe that they have the necessary authority, independence, and access to the CEO and the BoD. At the same time there are indications of certain shortcomings:

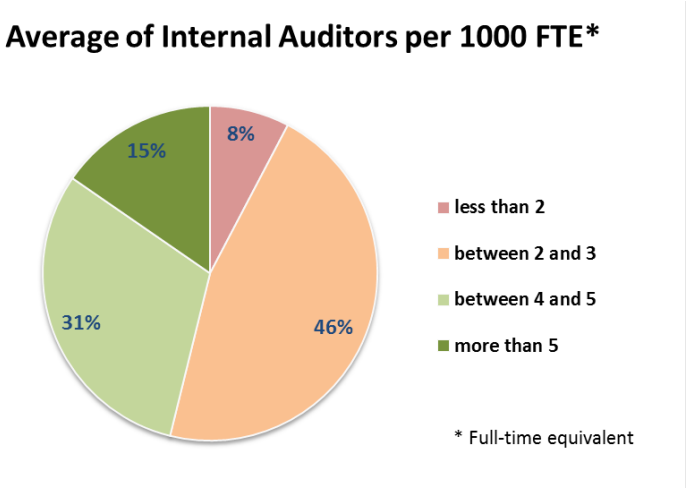
- Some Internal Auditors are not reporting sufficiently in person to the BoD (or its Audit Committee) but mainly via a written report. This limits the ability for interaction and discussion on audit points and deprives the BoD from the opportunity to see the Internal Auditor “live” and assess his or her effectiveness.
- In some foreign subsidiaries of Swiss insurers, the local internal auditor still reports functionally to the local CEO, though where this is due to local legal requirements these insurers are now taking other measures to preserve the local internal auditors’ independence.

[8] Functional or substantive reporting refers to who evaluates the performance of the Head of Internal Audit and determines bonuses, salary increases, employment termination, etc. - all factors which can influence independence and effectiveness. Administrative reporting relates to who approves expense reports, vacation requests, and other administrative issues not having to do with the substance of the work done by the Internal Auditor.

c. Questions on resources

The resources available to Internal Audit Functions vary widely among insurers, even after taking into account differences in size and complexity.

While the number of employees at a company is only a partial indicator of the internal audit needs of an insurer, it is noteworthy that differences in the number of auditors per 1000 employees can be significant. Whereas 15% of insurers have more than 5 auditors per 1000 employees, some insurers have less than 2 and 46% have between 2 and 3.



How budget and resources for Internal Audit are determined also raises questions at some insurers.

- It is not always clear if budget and resources are determined on a risk basis and take into account the strategy and multi-year audit plan of the Internal Audit Function.
- At some insurers the BoD or its Audit Committee appear to have relatively little say on the internal audit budget which is determined and approved at the Management level (e.g. by the CFO or CEO). The ability of the Internal Audit Function to influence its own budget is limited at some insurers.

Resource constraints at some insurers appear to have direct impact on the work of the Internal Audit Function, limiting what can be audited or with what intensity or regularity:

- Where resources are particularly small, the audits carried out appear insufficient to cover all major risk areas.
- In some cases audits that at some insurers are done in a cycle of every 1 or 2 years, at other insurers are done at larger intervals.
- The funds available for on-going training of internal audit staff can be minimal or non-existent.
- Budgets can also impact the quality of personnel that can be recruited and thus the quality of the audits conducted.

d. Some inconsistencies on basic practices

i. Although most insurers have an internal audit charter, not all are approved by the BoD or are reviewed often enough

In line with accepted practice, most insurers have a governing document for the Internal Audit Function in the form of a charter. However, not in all cases has this charter been approved by the BoD or its Audit Committee. In some cases – including at some Groups – the internal audit charter has not been reviewed for several years.

ii. Not all Internal Audit Functions are monitoring and measuring sufficiently their effectiveness or undergoing external reviews frequently enough

While most internal audit functions do some follow-up monitoring of their audit work, only some have developed robust key performance indicators or other means to measure qualitatively and quantitatively the effectiveness of a) their own function and b) their audit activity. For example, less than half of the internal audit functions are tracking sufficiently systematically the implementation by Management of their audit findings.

> One emerging good practice at some insurers is using timely and successful implementation of audit findings as one measure by which a senior manager's performance is assessed.

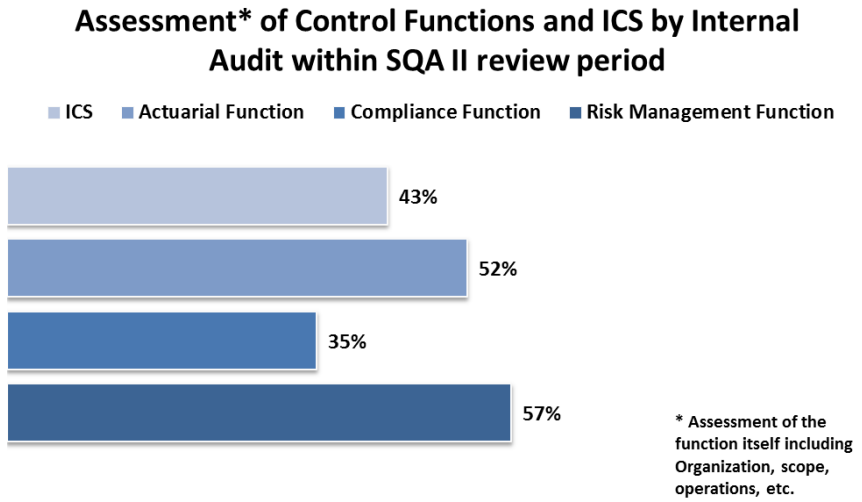
With respect to external reviews of the Internal Audit Function, the vast majority of insurers are following the Institute of Internal Auditors' standard of having such a review done at least every five years. However, some 15% of Internal Audit Functions have not had such a review in the last five years and, until the SQA II review pointed this out, were not planning to have one.

iii. Regular review by Internal Audit of other Control Functions is lacking

The periodic review by Internal Audit of other control functions (i.e. the assessment of the function itself including organization, scope, operations, etc.) is an important part of the assurance process at an insurer.

During the SQA II review period, some 60% of Internal Audit functions carried out such reviews of the Risk Management Function and 50% of the Actuarial Function. For the Compliance Function, the percentage is much lower. Also low is the percentage of Internal Audit Functions that have reviewed the Internal Controls System.

One concern relating to the above reviews is some uncertainty about scope and quality. It is not clear, for example, whether in some instances the Internal Audit Function is reviewing specific areas (e.g. anti-money laundering policies), which is important, but not the overall effectiveness of the relevant function (e.g. in this case, the Compliance Function).



iv. Some shortcomings in subsidiary-group relationship

Some insurers that are part of a Group have "insourced" their Internal Audit Function to the Group. While this can bring some advantages, including more independence for the internal auditors involved, it requires additional steps to ensure that the needs of the subsidiary in question are properly met. In some cases there is insufficient clarity as to whether:

- an appropriate part of the Group Internal Audit budget and resources is being dedicated to the subsidiary;
- the assigned internal auditors spend sufficient time at the subsidiary to know its business and risks;
- the assigned internal auditors (or the Group Head of Internal Audit) also report to the BoD of the subsidiary and not just to the BoD of the parent;
- the risk assessment and audit planning at the Group level takes sufficiently into account the peculiarities of the subsidiary and gives sufficient attention to risks which may not be material at the Group level but are at the subsidiary level;
- audit activity is designed and carried out in a manner that sufficiently takes into account local regulatory requirements.

e. There are some development needs for Internal Audit Functions

i. Many but not all Internal Audit Functions demonstrate a sufficiently strong improvement mindset

A majority of the reviewed Internal Audit Functions demonstrate a healthy self-critical view, have identified development needs and have action plans to address them. These tend to focus on:

- building up or re-enforcing the Internal Audit staff

- improving staff expertise in specific areas (such as IT, actuarial, governance, and finance)
- developing further the methodologies, tools and processes for Internal Audit
- putting in place proper succession planning.

However, at some insurers the Internal Audit Function shows insufficient reflection on where improvement needs exist or where they would like to take their function for its next stage of development. In such cases, these functions could run the risk of falling behind and diminishing their effectiveness over time.

ii. Within some Groups, there is a need to improve the enterprise-wide management of internal audit resources

There has been significant progress at most Groups in creating enterprise-wide audit standards and increasing the ability of the Group head of Internal Audit to assure more consistent audit quality across the Group. However, in some cases further work is needed in areas such as:

- formalizing the authority of the Group Head of Internal Audit in respect of local internal auditors
- ensuring that decisions on hiring, dismissal, promotion or demotion of local auditors are not made by local management, except where local law may require otherwise
- ensuring that the Group Head of Internal Audit is responsible for or is a main determinant of the performance evaluation of local auditors and of their compensation

iii. Internal Audit Functions want to increase impact of audits performed

Whether in Groups or Solos, many internal auditors express a desire to improve their audit work (processes, methodologies, resources, audit reports, etc.) in a way that has more impact within the company. For example by:

- improving risk assessments and audit planning such as to pinpoint better where internal audit work is most needed;
- improving the quality of their audits and analyses;
- strengthening the follow-up process of completed audits to ensure that agreed remediation actions are implemented;
- improving coordination with other Control Functions.

7. ACTUARIAL FUNCTION

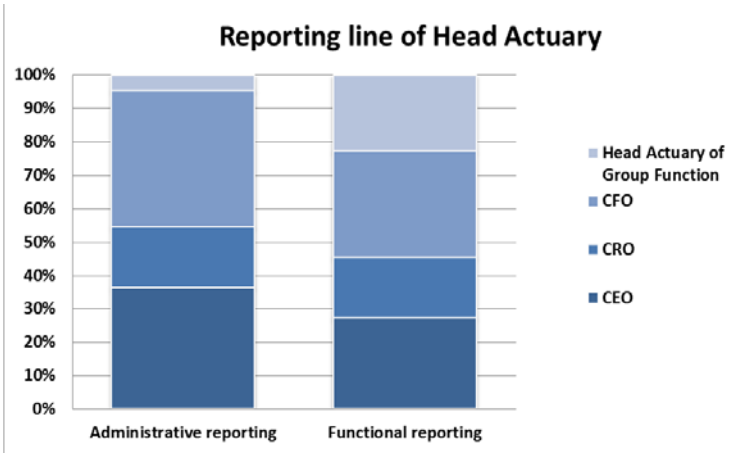
a. More coordination of actuarial activities is taking place at many insurers

SQA II covered primarily factors that can influence the quality and objectivity of the actuarial policies, processes, and information at insurers. It was not focused on the function of the Appointed Actuary.

SQA II shows that many insurers are working to better coordinate their actuarial resources enterprise-wide and improve actuarial performance, in some cases by having a Head Actuary (Chief Actuary or similar). In Groups, such efforts are also aimed at increasing the independence of local reserving actuaries which some Groups indicate still needs improvement. At smaller insurers the Head Actuary sometimes serves also as the Appointed Actuary, whereas at larger insurers it tends to be a separate and often more senior individual.

The role and authority of the Head Actuary differs across companies. At some insurers, the position includes overall functional responsibility for all actuarial matters and staff. In such cases, the ability of such a person to promote the independence of actuaries in separate units or legal entities and better quality and consistency appears much higher.

Reporting by the Head Actuary differs across insurers. At over 60% of insurers, functional reporting is now to the CEO or the CRO or, in the case of subsidiaries, to the Group's Chief Actuary. Functional reporting by the Head Actuary to the CFO, which can create certain independence and other challenges, takes places at about 30% of insurers.



b. Inconsistencies on actuarial policies and guidelines

While most insurers have developed written internal actuarial policies and guidelines which apply to the activities of their actuarial staff, a sizeable minority have not. Of these, some simply use applicable laws and regulations as a reference. Moreover, many of these do not hold regular training for actuarial staff.

By not having appropriate internal policies and guidelines and regular training, an insurer runs the risk of inconsistent interpretation and application by their actuarial staff of such laws and regulations.

Among the companies that do have actuarial policies or guidelines, some have made less progress on implementing these enterprise-wide. While some challenges arise due to differing local legal requirements, some companies successfully demonstrate that this does not impede having a consistent policy for those actuarial and quality assurance processes that are not affected by differences in local legal requirements.

c. Wide differences in actuarial information reporting

There is a wide range of practices in the upward reporting that takes place on actuarial information. At some insurers, the Head Actuary makes periodic reports directly to the BoD or a BoD committee. At others, the reports are limited to the MB or to a Management-level committee, while at a few insurers the extent of any regular upward reporting is less clear.

d. Management-level committees are being used to buttress the Actuarial Function

Groups in particular are increasingly using reserving or similar committees at a Management level to provide a governance framework around key actuarial-related matters. This usually includes the effectiveness of reserving methods, the quantification of reserves and reserve reporting. However, such a committee may also provide overall oversight of actuarial policies and practices.

Often such committees have representatives from different functions, such as the CRO, the CFO, and the CEO. The Chief Actuary sometimes but not always serves as the Chair of such a committee.

e. Challenges remain for the Actuarial Function

i. More segregation of duties is needed to avoid conflicts of interest and increase control role

At some insurers, those actuaries responsible for solvency, tied assets and reserving also have responsibilities for aspects of product development, pricing or underwriting or are otherwise involved in activities that may lead to conflicts of interest.

> Insufficient segregation can also adversely affect the actuarial control role and authority. This arises at insurers where the Head Actuary, for example, reports to the head of a business unit or to someone else carrying out a business operational role.

A stronger recognition of its control role can help the Actuarial Function in reducing the chances of actuarial opinions or recommendations not being taken sufficiently into account or being overridden by Management without appropriate BoD review.

ii. More effectiveness of the Actuarial Function is a goal

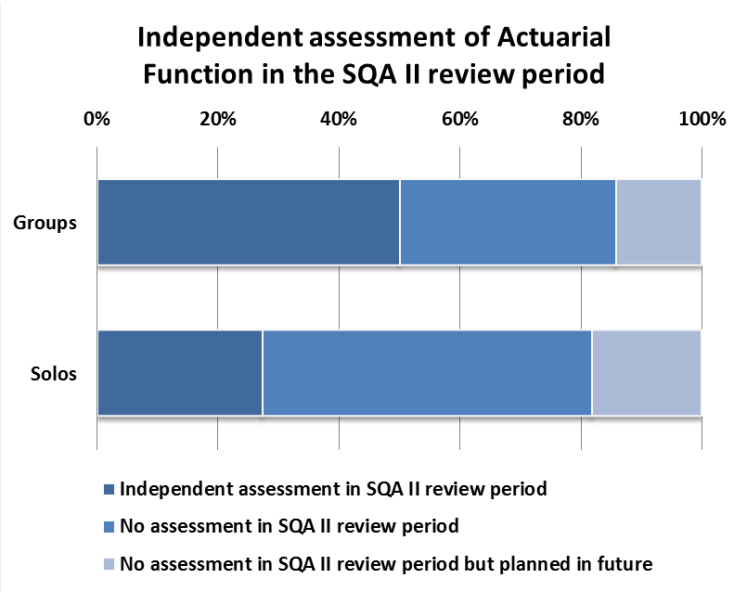
Many actuarial functions see a need to improve effectiveness such as through:

- better processes, systems, models, and tools
- strengthening actuarial know-how
- more resources
- increasing the overall ability to meet accounting and solvency rules.

f. Assessments of Actuarial Functions still insufficient

Most insurers (including Groups) are not measuring sufficiently the effectiveness of their Actuarial Functions. When assessments are done, they tend to be informal, irregular, or limited to a specific actuarial issue, rather than involving a full evaluation of the function. There appears to be also limited reporting on the performance of the Actuarial Function to the CEO, the Management Board or the BoD.

Formal independent reviews of actuarial functions (e.g. by Internal Audit or an external party) are becoming more frequent, but are still low (only 40% of insurers have had or are planning such a review). The percentage is higher among Groups.



8. COMPLIANCE FUNCTION

a. Compliance sensitivity appears to be increasing

i. More Management awareness but clearer compliance priorities need to be communicated

The SQA II assessments suggest greater Management interest in the compliance area at many reviewed insurers. This appears to be the case also on the part of the CEO to whom Compliance Officers are gaining increasing access.

One area of increased compliance activity relates to cross-border risks. Most insurers report being exposed to such risks in some way. They indicate devoting more time to this area, in each case with the involvement of the Compliance Officer. Some insurers are cutting back their cross-border business activities to reduce these risks.

To give better focus on compliance about half of all insurers now have a Management-level Compliance Committee or similar or have a Risk Committee where the Compliance Officer is represented. A Compliance Committee or similar at the local Business Unit level is present in around one quarter of insurers.

Perhaps due to an increased appreciation of the need to manage compliance risks closely, the percentage of insurers which outsource the Compliance Function is low (some 10%). Some insurers outsource specific compliance tasks, such as data protection or internal fraud. But these instances are less common.

However, not all insurers are clear in the internal messaging on compliance and risk taking.

While some insurers are specific in communicating that their company has a policy of zero tolerance on compliance violations, others either do not address this point or communicate in a way that may create the impression that employees may take compliance risks in some cases. For example, some insurers still do not provide employees direct guidance that in the case of a conflict between a business goal and a legal or regulatory obligation, the latter takes precedent.

ii. Codes of conduct are now prevalent; some show room for improvement

All reviewed insurers (except one) have a Code of Conduct in place, though some were developed only in the past two years. Over half of insurers have updated their Code of Conduct recently or are currently revising it.

There is evidence that insurers are taking pro-active steps to promote familiarity with the code of conduct. Some examples include:

- Nearly all insurers have the Code of Conduct on the company intranet (though it is not clear if at all insurers this is done prominently enough such that employees are reminded regularly and can easily access the Code of Conduct).
- Some 50% of insurers require all employees to periodically acknowledge in writing their familiarity with the Code of Conduct, while some 10% require this only of those employees who may impact the company's risk profile (Key Risk Takers).
- Approximately half of insurers conduct periodic training for the BoD and for Key Risk Takers on the Code of Conduct.

Compliance officers in general find their Code of Conduct to be adequate, though some see a possibility of improvement in terms of:

- making the Code of Conduct more user friendly and less technical and legalistic
- including practical examples of appropriate and inappropriate behaviors
- mentioning the existence of the Compliance Function in the Code of Conduct itself
- incorporating references in other key company documents to the Code of Conduct and vice-versa
- enhancing the values and ethics components of the Code of Conduct

The last point relates in general to a broader challenge which many but not all insurers have begun addressing in their compliance efforts. This is the challenge of integrating more effectively the Code of Conduct and all the compliance efforts into the insurer's culture and establishing a more direct connection to the business strategy.

b. BoD engagement on compliance less visible

As indicated earlier, BoD oversight of risk in general appears to be higher but it is unclear if this also extends sufficiently to cover compliance and related topics.

For example, only about half of insurers with a Compliance Function strategy have had it formally approved by the BoD. BoD approval of the Code of Conduct and other important compliance policies is not clear at some insurers. Moreover, some BoDs appear not to be providing a direct 'tone from the top' on the importance of compliance and ethical considerations.

At some insurers, the interaction of the BoD with the Compliance Officer remains limited. In some cases, the Compliance Officer is not reporting directly to the BoD. In other cases, even when such reporting takes place, it is not clear if it is supplemented with other interactions (such as separate periodic meetings between the Compliance Officer and the Chair of the Audit Committee or the Chair of the BoD). And only a few BoDs require being consulted in any dismissal of the Compliance Officer.

c. Shortcomings remain in compliance structures

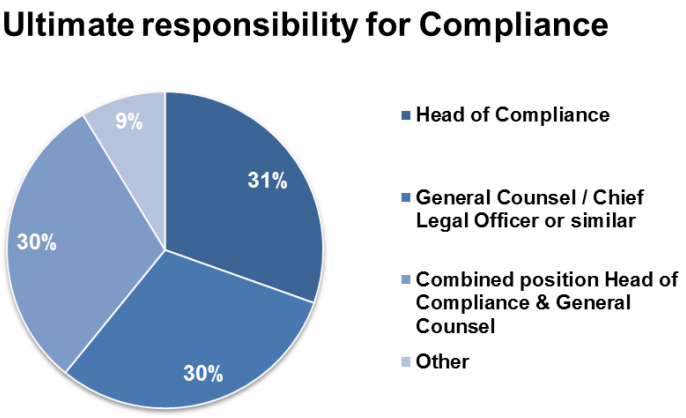
i. Increased recognition of compliance as distinct area but more work is needed

Nearly all insurers now have a Compliance Officer. This is a clear improvement over SQA I where many insurers lacked such a function or, in some cases, showed a limited understanding of why such a function is needed in the first place.

While at the majority of insurers the Compliance Officer is now a separate position, at others it is unclear if it is a legal counsel who has been given an additional title.

To provide compliance more focus and less co-mingling with traditional legal activity, some insurers, including three Groups, are establishing Compliance as a distinct and separate unit or are putting it outside the legal function, such as part of the Risk Management Department or under the company's Chief Administrative Officer or similar.

One result of the above trends is that some 30%[9] of the Heads of Compliance now have ultimate responsibility for Compliance, rather than such responsibility being assigned to the General Counsel or another person. This means that most Heads of Compliance still do not have direct accountability to Management and the BoD.



The above shortcoming is mitigated by the fact that some Heads of Compliance who do not have ultimate compliance responsibility still make their reports directly to the BoD. For the rest, however, the consequence is that the BoD does not have the opportunity to hear directly the views of the Compliance Officer or question him or her directly on areas of concern.

One positive trend is a reduction in the number of Compliance Officers also carrying out a business role or other activity that may generate a conflict of interests. A few such examples remain (e.g. the head of

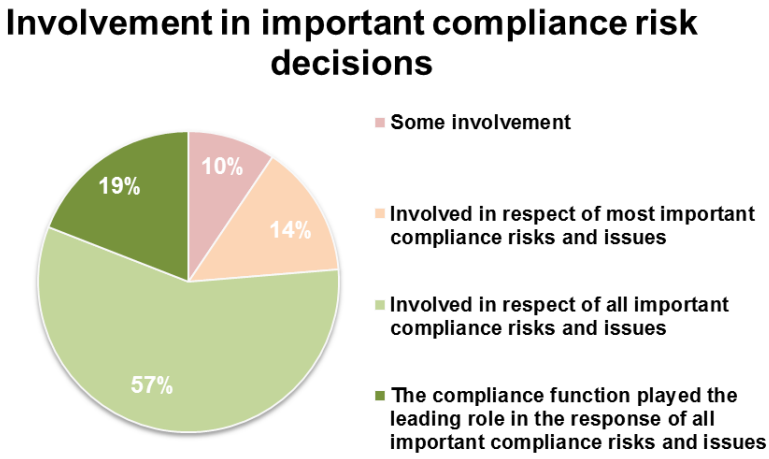
[9] This figure does not include the approximately 30% of General Counsel who simultaneously act as Compliance Officer.

underwriting also serving as Compliance Officer or the Compliance Officer also being involved in certain investment-related activities).

ii. Some Compliance Officers still have limited scope and authority or the authority is not sufficiently documented

While the scope and authority of Compliance Officers appears to be increasing, at some insurers these remain more restricted.

For example, some 25% of Compliance Officers indicate not being involved in all important compliance risks decisions at their company.



At a few insurers, the Compliance Officer's scope is truncated, for instance limited to reviewing risk transfer limits. At other insurers the scope is larger but still may exclude certain areas of legal or regulatory importance.

At some insurers, the Compliance Officer's scope is adequate (covering, for example, legal and regulatory compliance in general as well as ethical matters) but the authority is not appropriately documented. To bring clarity some insurers have defined authority tables indicating when the Compliance Officer has decisional authority and when he or she has to be consulted or informed.

While some 20% of Compliance Officers deem both their authority and how it is documented to be state of the art, a comparable percentage considers both to be insufficient.

At about 20% of insurers, the reports from Compliance to the BoD are subject to Management pre-approval.

d. Progress on compliance policies but compliance strategies still not well developed

i. More compliance policies are in place, though it is not clear if their effectiveness is sufficiently tested

The SQA II assessments suggest that insurers have intensified their efforts on compliance policies, including broadening them to cover new risks such as social media.

> The most common compliance polices are in the areas data protection, competition, anti-money laundering, insider trading, trade sanctions, cross-border risks, and anti-bribery/anti-corruption.

With respect to anti-bribery / anti-corruption, most Compliance Officers confirm that their companies have a clear top-level company commitment against this. Also the majority indicate that this commitment is now accompanied by guidance on acceptable and non-acceptable practices.

In general Compliance Officers believe their policies are effective, though it is unclear the extent to which testing and auditing for effectiveness is taking place.

ii. Further work is needed on compliance strategies and operational plans

A written strategy for the Compliance Function is critical for long-term direction and to ensure there is institutional agreement, including at the highest level of the company, on the compliance strategic priorities.

Nearly 65% of insurers now have a documented compliance strategy (the percentage is higher at Groups). However, at 70% of insurers such a strategy has not been approved at BoD level and at only 40% has it been approved at the Management level (either by Management Board or the CEO). At 30% the strategy has received no top level approval.

There is a wide gap in the adequacy of the articulation of compliance strategies. Some strategies appropriately set the direction for the function, while others are too generic or otherwise are such as to not provide an adequate sense of what Compliance aims to accomplish long-term.

To implement the compliance strategy, 60% of insurers now have established compliance operational plans, on a yearly or other periodic basis. The quality of the operational plans also varies, with some Compliance Functions lacking measurable goals or targets.

e. Greater attention needed on customer-focused compliance and on conflicts of interest

i. Sufficient customer-focused compliance lacking in some cases

The Compliance Functions of insurers involved in selling personal lines indicate being involved in the 'suitability' area, i.e. the review of the appropriateness of products sold to consumers in light of their specific circumstances. The importance of this is highlighted by the fact that of those insurers involved in

personal lines, approximately 20% have actually faced legal or other proceedings relating to suitability in other jurisdictions.

All the same, other indicators suggest that more Compliance involvement is needed in the customer area:

- Only some 40% of insurers involved in personal lines analyse customer complaints to identify potential compliance issues and trends. Such reviews can be instrumental for remediating any compliance issues promptly and before they escalate into legal liability.
- 30% of insurers still do not involve the Compliance Function in the review of new products or major changes to existing products.

ii. Conflict of interest processes need strengthening

Since conflicts of interest can arise in many different forms and at all levels (from the BoD level, down to the employee level), it is an area of exposure for all companies. This is also the case when looked upon from the perspective of internal conflicts (such as when one person is asked to exercise incompatible roles) as well as external conflicts (such as in relationship to suppliers, customers, etc. or when a BoD member or an employee carry out external activities that conflict with the interests of the company).

While over 80% of insurers have conflicts of interest policies, it is not always clear whether these policies have been reviewed recently to ensure they address the various types of conflicts that may arise at their company in today's environment.

Only 40% of insurers reviewed have carried out a conflicts of interest risk assessment and 30% have no specific compliance processes for identifying, assessing, and resolving conflicts of interest. At some insurers the matter is left up to the line managers without appropriate Compliance support. At some 15% of insurers the Compliance Function is not involved at all in conflicts of interest reviews.

f. Evidence of good practices but also of on-going improvement needs

Many Compliance Functions are following numerous good compliance practices such as:

- *Planned Senior Management Access:* regularly scheduled individual meetings in the course of the year between the Compliance Officer and each member of the MB to review compliance matters in that member's areas of responsibility.
- *Compliance Inventories:* a register of the key legal and regulatory obligations that the insurer faces, with specific mapping of the resulting obligations and clear allocation of who at the company has main responsibility for these. One quarter of insurers do not have such inventories.
- *Involvement of the Compliance Function in important transactions:* Over 80% of insurers report such involvement.

- *Review of fines and costs incurred due to non*-compliance: nearly half of insurers have processes in place to track such fines and costs and use them to improve compliance at the company.
- *Litigation roster review:* Some 60% of insurers review the list of litigation in which the company is involved to draw relevant compliance lessons.
- *Employee surveys:* over 80% of insurers use employee surveys to obtain confidential employee input on compliance, particularly on the Code of Conduct.

Improvement needs remain in a number of key areas at many insurers such as:

- improving the documentation of authority and independence of the Compliance Function;
- ensuring that adequate and appropriate reporting lines are in place;
- granting the Compliance Function more input on its budget;
- development and use of reliable key performance indicators;
- more review of the effectiveness of the Compliance Function (52% of insurers have not done such a review);
- better communication on compliance: some 20% of insurers still do not have a special compliance site on their intranet to better communicate with employees and, of those who do, only one fifth track its usage to determine if employees are being reached;
- benefiting from the views of departing employees (e.g. through the use of exit interviews to obtain input on how compliance efforts could be improved or regarding any company practices that are not consistent with the internal compliance and risk policies).

9. COMPLIANCE-RELATED RISK AREAS

a. Anti-Money Laundering / Anti-Terrorist Financing (AML/ATF) mechanisms are in place but many remain basic

In light of the higher risk in life insurance AML/ATF efforts are more prevalent in this sector. However, insurers in other sectors are also recognizing potential exposures and are taking measures.

The higher risk of cross-border business is being recognized by insurers. For example, less than 15% of reviewed insurers now offer life insurance wrappers. Only about 5% indicate that their AML/ATF risk profile has increased considerably in the previous two years. Many insurers also see their net risk profile improving after mitigants are applied, which would suggest effectiveness of these mitigants.

Some insurers are using advanced AML/ATF methodologies, such as risk modeling, and are turning to more IT solutions. At other insurers it is less clear how the efficiency of processes is being improved without appropriate IT gains. Nonetheless, nearly all insurers judge their approaches as adequate. Among larger insurers three quarters judge their AML/ATF function itself as “good” or “very good”.

Whether these figures represent a degree of over-estimation is not clear. Some questions do arise, particularly at Solos, regarding the positioning of the Anti-Money Laundering Officer and his or her ability to be effective. For example, at some insurers instead of being part of the Compliance Function, the Anti-Money Laundering Officer reports to a business line manager, who is sometimes of the very same division for which the anti-money laundering officer is responsible.

There are signs of more AML/ATF activity, particularly among larger insurers. Among these, some 60% indicate having carried out significant AML/ATF projects in the previous two years.

Areas where specific improvement needs appear to remain at some insurers include:

- Better Group-wide coordination and oversight of AML/ATF efforts, particularly in companies with foreign activities.
- Reporting on AML/ATF to the BoD is limited. For example, even among larger insurers only about half report to the BoD statistical data on trends in suspicious transactions and the relative exposures of the insurer's units and products.
- Better training in the AML/ATF area.

Insurers will need to continue giving high attention to the AML/ATF area. In addition to the possibility of AML laws tightening further in Switzerland, there is the risk of insurers being increasingly targeted by money launderers who are looking for alternative means of placing their money.

b. Preventing insider trading: widespread use of policies but scope and preventive measures vary widely

Most insurers (over 80%) have in place an insider trading policy. The awareness of the risks that can arise from insider trading is also reflected by a number of other positive practices some insurers are following. These include:

- Requiring approval by the Compliance Function before an employee or BoD member may trade in the securities of the insurer. In some cases this involves the Compliance Officer interviewing the person.
- Setting closed periods during which such trading is prohibited, such as near to the publication of financial results or during price sensitive projects.
- Setting closed periods for a long enough period of time, sometimes well over a month, prior to the publication of financial results.
- Covering in the insider trading policy close family members or those living in the same household to prevent imputed knowledge if such persons trade during times when it is prohibited for the employee.
- Complementing preventive efforts with detective methods to verify that insider trading policies are being adhered to.

However, other insurers only have a policy and demonstrate few compliance implementation processes. Further, some insurers are only covering the risk of employees using non-public information learned on the job to deal in their own company's securities (when the company is publicly listed) but not in the securities of other companies (such as corporate clients of the company or companies in whose securities the insurer invests).

Other weaknesses observed at some insurers include:

- too narrow a scope of their policy, for example failing to cover Board of Director members;
- insufficient communication or training on insider trading prevention;
- little involvement by local Compliance Functions in actively supervising the insider trading policy locally;
- insufficient effort in assessing where weaknesses may exist or improvements may be needed.

c. Policies for employees to report concerns or violations are increasing but there are insufficient efforts to optimize

Some employees who have a risk, compliance or ethical concern or who are aware of actual violations may hesitate reporting this. This may occur, for example, if they fear it may not be taken seriously by the company or that they may be considered disloyal for reporting it. Fear of possible negative consequences for their employment may hold back some employees from reporting legitimate issues.

Insurers appear to recognize increasingly that employees constitute an important source of information about matters that, if timely reported, could protect the company's assets and reputation. Some four out of five insurers now have an employee reporting or similar policy and some 65% of these offer the option of anonymous reporting.

However, not all employees accompany this policy with concrete mechanisms to facilitate this reporting:

- Only a minority of insurers include an express anti-retaliation clause in their reporting policy; this can be a significant weakness as employees who report may fear reprisals without this clause.
- Not all insurers have a specific confidential telephone hotline, fax or internet platform for employee reporting. In general, larger and internationally-active insurers tend to have more advanced means in this respect or may use an external provider.
- Some insurers limit what employees may report. Some do not include concerns but only violations. Some cover only violations of laws but not of internal policies (such as risk policies). Others limit it to one area only (e.g. fraud, financial violations, etc.).
- Only a minority of insurers are using the information from employee reporting to conduct diagnoses of possible areas of weakness within the company.

In general, insurers report very limited usage by employees of the reporting mechanisms. This may be due to a variety of reasons. For example:

- employees may not know that a confidential reporting mechanism exists;
- employees may sufficiently trust and use other avenues available to report issues, for instance, their managers or the Compliance Officer, such that they don't see a need to use the confidential reporting mechanism;
- few issues arise at the insurer that prompt employees to report;
- employees do not have confidence in the reporting mechanisms, fearing for example that confidentiality or anonymity will not be honored or that they will be subject to retaliation.

Due to the above some insurers are conducting periodically employee surveys to assess the extent of employee familiarity with and confidence in the reporting systems and, based on these, are making needed improvements.

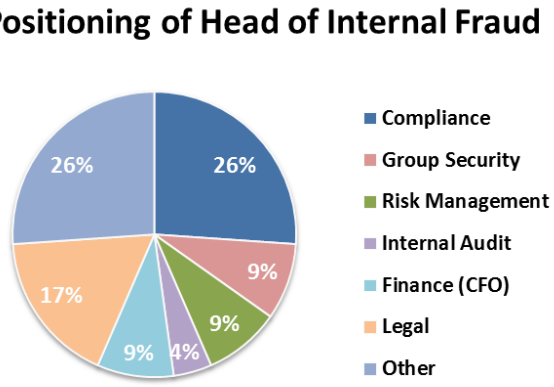
d. Internal fraud prevention generally moving on right track but intensified efforts are required

No company is exempt from the potential of a rogue manager and other employee committing a fraud against it.

Many insurers appear to be taking this risk more seriously. They are developing internal fraud strategies and strengthening messaging on internal fraud, such as indicating non-tolerance of internal fraud and a commitment to report to authorities for prosecution cases of internal fraud.

The efforts appear higher among Groups. Some Solos show little activity. Most reviewed insurers have a fraud risk policy, either stand-alone or part of another policy and almost all have a designated person for internal fraud.

At most insurers the person responsible for internal fraud prevention is located in a non-operational function such as Compliance, Legal, Risk Management or Group Security. However, in some cases the responsibility for internal fraud prevention lies with a function that itself is exposed to internal fraud, such as Finance, or that otherwise has business operational responsibilities. This could give rise to conflicts of interest and diminish the effectiveness of the internal fraud efforts.



Another non-optimal practice is assigning the Internal Audit Function operational responsibility for internal fraud prevention. This creates the uncomfortable situation of Internal Audit having to audit its own efforts on internal fraud and forces Internal Audit into an implementation role which is not compatible generally with its assurance mission.

Many insurers are conducting fraud-specific internal audits. However only half have a formal process with steps to follow in case a suspicion of an internal fraud arises. The rest do this ad-hoc.

Other areas where more emphasis may be needed at some insurers include:

- programs to increase employee awareness of internal fraud;
- risk assessments to identify preventively areas, units and personnel that may be more subject to potential internal fraud;
- developing forward-looking internal fraud risk indicators;
- mining data to identify potential risk trends;
- better internal exchange of information and coordination on internal fraud among the different parts of the company;
- better reporting on internal fraud to Management and to the BoD;
- more effective controls, including detective controls.

10. EMPLOYEE TRAINING

Compliance and risk training: a strong development need

SQA II reviewed insurers in terms of employee training in compliance and risk management topics. This emerges as the area with the lowest assessment for nearly all insurers, including Groups.

> Training objectives could include, for example, ensuring that the top five key areas of risk and obligation of the insurer are covered at a defined frequency for a defined employee target population. It could also focus on increasing employee skills measurably in critical areas, such as on competition law or IT-security risk. Or it could include, for instance, ensuring that 100% of new employees receive Code of Conduct training before their third month on the job and that existing employees receive such training every two years. Alternatively, it may require intensive compliance and risk training for the most senior managers or those in positions with particular exposures.

Very few insurers demonstrate having a training strategy or long-term plan in the above areas. While there is evidence of training activity, training decisions appear more ad-hoc rather than in accordance with well-defined objectives.

In terms of coverage of training, the SQA II assessments suggest there are gaps in some instances. While an insurer might have training in money laundering, it may lack training in data protection. Or while an insurer may cover adequately compliance topics, it may offer little training in the risk management areas. In general, there is less evidence of risk training than compliance training.

Nonetheless, even in the compliance area there appear to be weaknesses. For example, few insurers hold training on insider trading, conflicts of interest, and competition law, for example. In general, Solos do less well than Groups on training.

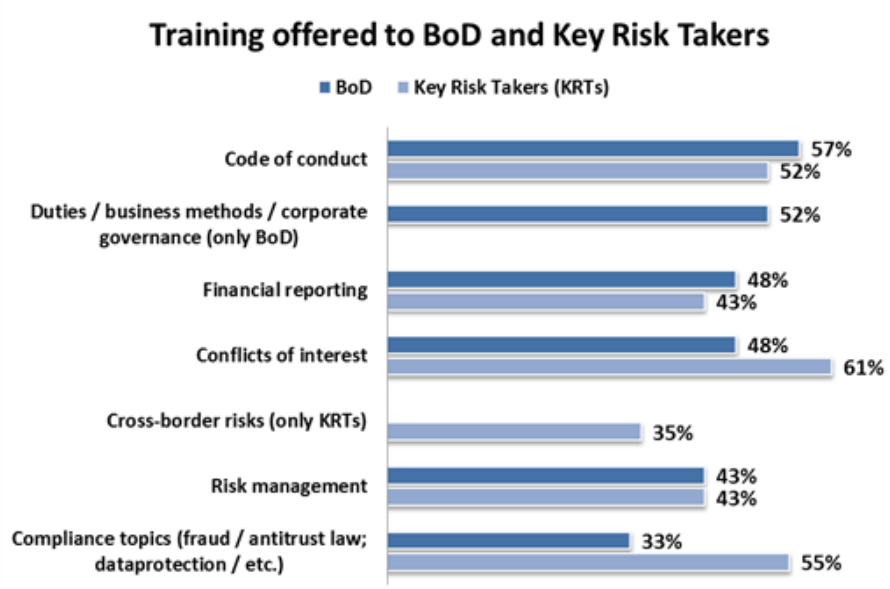
Other common weaknesses found:

- **Lack of structure.** Training without specific learning goals or structure; mere presentations sometimes labelled as ‘training’.
- **Insufficient regularity.** For important subjects the last training sometimes goes back years.
- **No measurement**. Little evidence that the impact of training held is assessed, including in terms of learning effectiveness by the participants and effect on the observance of compliance and risk policies.
- **Limited Group-wide view.** Groups do not always monitor what training is done at local levels and lack thus a Group-wide view on the adequacy of training in the compliance and risk areas. It is also unclear if Group-wide training requirements exist such as to provide more assurance that Group-wide policies are understood and will be complied with at local levels.
- **Little impact of non-participation.** At only 30% of insurers is the non-participation of an employee in required compliance and risk training considered in the employee’s performance evaluation.

A few positive trends in training were found:

- Four out of five Groups now offer training on their Code of Conduct; the proportion is significantly lower among Solos.
- More insurers are using the concept of Key Risk Takers and some appear to use this as a criterion for focusing training.
- Some 70% of insurers are providing the BoD reports on their training efforts, though the regularity, content and quality of such reports is not clear.

Looking ahead, insurers appear to recognize the need for improvement. Many insurers expect to give more focus on training, with increased use of web-based learning and other forms of e-learning.



11. OUTSOURCING

Governance and risk assessments of outsourcing: a potential weakness area

SQA II did not review what insurers outsource, but which governance and risk arrangements exist for their outsourcing activities. This is an SQA II area in which, after employee training, insurers in general show the least strength.

In some cases, this may have to do with the fact that some insurers undertake little outsourcing. Furthermore, no reviewed insurer anticipates any major increase in its outsourcing in the near future. Nonetheless, the SQA II assessments suggest insufficient attention among many insurers to the potential risks of outsourcing and insufficient oversight of the area, including from the BoD.

Only about half of insurers have an outsourcing policy, with no major differences as between Groups or Solos. Only about one third of those insurers that have an outsourcing policy have had it approved by the BoD, and only 40% of all insurers have any regular reporting to the BoD on outsourcing activities.

Other common shortcomings in the outsourcing area include:

- lack of relevant thresholds for outsourcing above which appropriate approvals and reviews are triggered (some insurers have begun setting these, such as requiring BoD approval for outsourcing exceeding a certain financial level);
- not subjecting “insourcing” (delegation of tasks or functions to another entity within the Group) also to appropriate controls and reviews, including ensuring appropriate ‘arms-length’ conditions;
- while the Legal Function usually appears involved in the contracting process of outsourcing, there is less evidence of the Compliance Function and Risk Function being involved in reviewing the provider of outsourcing on its own risk management, compliance and internal controls systems or in requiring an external quality assurance certification in these areas;
- not having Risk Management conduct assessments of a) individual outsourcings before they are undertaken or b) the cumulative risk of all outsourcing activity; only about one third of insurers currently do this;
- insufficient reviews of outsourced activities by the Internal Audit Function;
- insufficient additional due diligence and assessments when the nature of the outsourcing involves higher risks such as offshoring or the outsourcing of key functions.