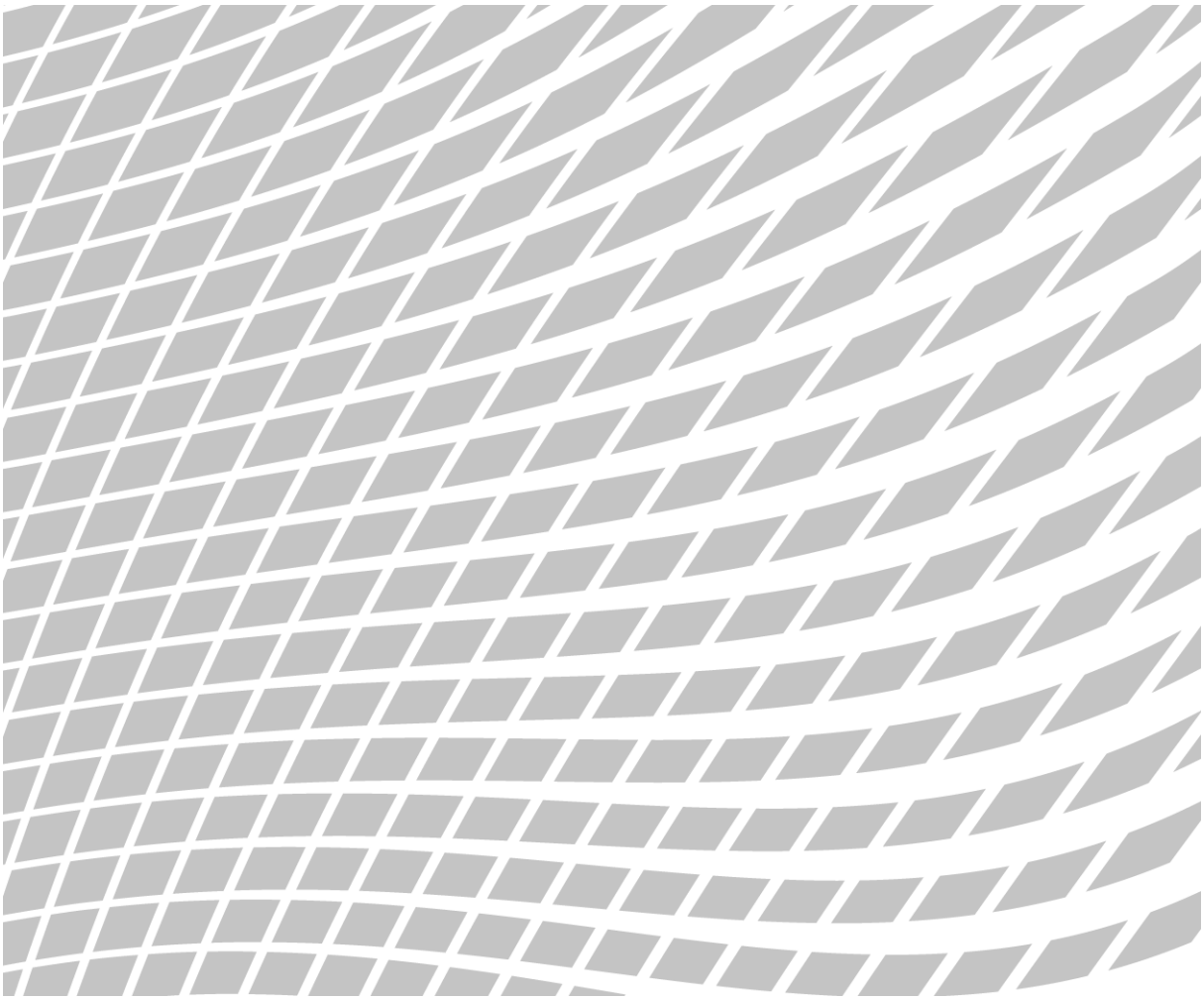
Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

1 February 2010

Governance, Risk Management and Internal Controls at Swiss Insurers

Observations from the first Swiss Qualitative Assessment



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

A276210/GB-G/G-KDI

finma

Table of contents

Glossary of Abbreviations Used in this Report

CG	Corporate Governance
CEO	Chief Executive Officer
CRO	Chief Risk Officer
MB	Management Board, Executive Committee or similar management body
ICS	Internal control system
RM	Risk management
Solo	an insurer which does not belong to a group
SQA	Swiss Qualitative Assessment
SQA I Submission	the answers, self-assessment, and documentation submitted by the insurers in response to the first Swiss Qualitative Assessment
BOD	Board of Directors

A. Introduction

This report is a summary of FINMA's key observations from the 2008 submissions of Swiss insurers under the first Swiss Qualitative Assessment (SQA I). The observations are based solely on these submissions. Progress made by insurers since then is not reflected in this report nor are the results of SQA risk dialogs held with certain insurers in 2009.

B. SQA I Basis and Methodology

As part of the revisions to the Swiss Federal Law on the supervision of insurers[1], insurers were required to adapt their corporate governance, risk management, and internal control systems to meet the requirements set out therein.[2] FINMA considers CG, RM und ICS as indispensable components for the sound management of a company. These areas in turn constitute key elements of qualitative supervision. Together with quantitative tools (for example, the Swiss Solvency Test) and with traditional supervisory tools (such as on technical reserves and tied capital), qualitative elements complete FINMA's integrated approach to insurance supervision.

In furtherance of the foregoing, the then Office of Private Insurance launched a survey among over 160 insurers which required completion by 31 March 2008.[3]

The information in the SQA I submissions provide FINMA helpful evidence of the various practices being used by insurers to implement corporate governance, risk management, and internal control principles. They also provide insights on how insurers perceive themselves in these areas. FINMA is using the results of its evaluation of the SQA I submissions to hold with selected insurers more focused discussions on these topics and otherwise to enhance its understanding of a company's risk profile. The results of SQA I are also assisting FINMA in setting supervisory priorities and developing SQA II.

[1] Versicherungsaufsichtsgesetz [VAG]; SR 961.01

[2] The supervisory practice thereto is contained in the "Circular on Corporate Governance, Risk Management, and Internal Control System" which came into effect on 1 January 2007 (RS 15/2006, now called FINMA-RS 08/32 of 20 November 2008).

[3] Insurers were asked to answer a questionnaire on CG and one on RM/ICS and to submit supporting documentation. Insurers were permitted to include all information they wished in support of their submission. Insurers answered by the required deadline or by an extended deadline granted in limited cases. Each questionnaire was constructed similarly. In the first part an insurer had to list and include relevant documents. In the second part it answered questions relating to its practices in the relevant areas. In the third part the insurer had to carry out a self-evaluation using the questions provided.

C. Purpose of this Report

As this report summarizes observations from all insurers that participated in SQA I, it provides a larger context for an individual insurer to assess its own practices. The report highlights certain areas where the SQA I submissions show good practices, insufficient clarity, or patterns of potential weakness. This should be of utility to each insurer in its efforts to further develop or fine-tune its individual CG, RM, and ICS approaches. It is important to note that not all good practices being followed by Swiss insurers are mentioned in this report, nor are all weaknesses.

D. Key Observations from SQA

1. Uneven Landscape

There is evidence of progress on CG/RM/ICS among Swiss insurers but not evenly across all insurers or in all areas of CG/RM/ICS.

Overall the SQA I submissions suggest that Swiss insurers are increasingly giving attention to the CG/RM/ICS areas and putting in place relevant structures and processes. However, there are marked differences among insurers in the degree of overall CG/RM/ICS preparedness as well as preparedness in specific areas.

The above observations remain true even when insurers of similar size are compared. Thus, there is a noticeable range of preparedness among larger insurers as a peer group, among mid-size insurers as a peer group, and among smaller insurers as a peer group.

Differences also exist within insurance sectors. For example, pronounced differences appear to exist among solo life insurers when these are compared as a peer group.

The above suggests that neither size nor sector alone is a determinant of how well prepared an insurer is in the CG/RM/ICS areas. A stronger factor appears to be the extent of BOD leadership in these areas and the strength of an insurer's control functions.

In addition, the SQA I submissions suggest that even within a single insurer there can be notable variations on preparedness in the various CG/RM/ICS areas. An insurer may show strength, for example, on risk reporting but not on risk identification or assessment. It may show relative financial risk management adequacy but insufficient efforts on compliance. Or it may show comprehensive policy manuals but little on how employees are trained on those manuals or on processes to implement the policies.

While smaller insurers have obvious limitations due to their size and sometimes very limited personnel, the SQA I submissions reveal that some smaller insurers are making considerable efforts to enhance their CG/RM/ICS preparedness. They also show other smaller insurers that appear to be lag-

ging behind and which may not be making sufficient efforts proportional to other insurers of similar size. The BODs, management, and the control functions of these insurers should give particular effort to reviewing if their company's activities in the CG/RM/ICS areas are sufficient in light of its risk profile and the legal and regulatory obligations applying to it.

Differences among group companies

SQA I submissions also reveal differences among entities part of the same group. In some cases this may be due to insufficient group standards in certain CG/RM/ICS areas. In other cases, it may have more to do with insufficient implementation at the single entity level.

For example, some entities belonging to a group enclose copies of group standards but do not demonstrate sufficiently the extent and quality of implementation of those standards at their level. This may be related to insufficient local resources, insufficient understanding of what is expected by the group, or insufficient supervision by the group. Either way, this is not only a problem of that entity. A single entity, even if small, could potentially create reputational or other risks for the entire group. Thus the deficiencies of a single entity should be of concern to the group. The group's BOD could consider requesting and monitoring information showing the comparative performance of the group's entities on various CG/RM/ICS indicators.

Gaps on basics

The SQA I submissions also reveal differences in some more fundamental areas. For example, the submissions of some insurers fall under acceptable levels in a very basic domain: governance documentation. At some of these insurers there are:

- Documents that have not been updated in many years or are not dated at all
- Absence of or inadequate organizational rules
- When not in the organizational rules, absence of a matrix or other document detailing the allocation of responsibilities and decision-making authority as between the BOD, the MB, and other bodies or key personnel of the company
- Absence of or inadequate charters for the BOD or MB committees and for control functions

Insurers should recognize that reasonable, quality documentation is needed not just as a legal housekeeping matter. Particularly when put in user-friendly form and made easily available to employees, appropriate documentation can help with the implementation of company CG/RM/ICS goals. It can contribute to execution consistency and to quality improvement. As a control matter, appropriate documentation is essential for the verifiability of policies, processes, and outcomes.

2. Sufficient Self-critique?

The SQA I submissions suggest that some insurers tend to overestimate their level of CG/RM/ICS preparedness.

In their SQA self-assessment a majority of insurers of all sizes indicate no or only modest improvement need in most CG/RM/ICS areas. This includes insurers whose SQA I submission suggests there may be certain weaknesses. Some insurers indicate that they already have reached appropriate practice in a particular domain but do not provide sufficient explanation or substantiation for this claim.

While FINMA is aware that for most insurers their SQA self-assessment is based on a good faith estimate and that legitimate differences of opinion can exist, it is concerned that some insurers may not be giving sufficient attention to critical self-analysis or to informing themselves sufficiently of market trends in the CG/RM/ICS areas. Failure to do this itself can be a governance weakness.

The BOD of an insurer should ensure that robust and candid discussions (also with management and the control functions) take place regularly to identify potential improvement needs. Bench-marking and testing internal practices against appropriate market good practices can help provide perspective and a more informed basis for determining if the company's CG/RM/ICS practices are adequate in light of market developments and the company's specific risk profile.

3. Positive Correlation of Governance to Risk Management

Insurers which appear more prepared on CG also appear more willing to try to do well on RM/ICS.

The SQA I submissions suggest there may be a positive correlation between CG preparedness and progress on developing RM/ICS. If the governance organs—particularly the BOD—are properly constituted and are operating with the right information and checks-and-balances, this would appear to create an auspicious setting for the insurer to work on developing or advancing appropriate RM/ICS systems.

If the above is true, the implication is that an insurer's BOD would wish to ensure as a first priority that a solid corporate governance infrastructure and approach are in place since this appears to provide a foundation for RM/ICS efforts. Equally important, the BOD should recognize that corporate governance is essential for providing formal legitimization of and authority for the RM/ICS and other control functions. For example, if the organizational rules of a company specifically mention the function of the chief risk officer and describe his or her powers and accountabilities, this provides beneficial governance anchoring for the CRO. This can help with his or her effectiveness and contribute to preventing, for example, that changes in management or management cost-cutting initiatives result in changes that adversely affect the CRO's ability to fulfill his or her duties.

The BOD, and particularly the Chairman, should take the lead for the insurer's overall governance health. In so doing the BOD it is also setting the foundation for proper risk management and for the corresponding control functions.

4. Open Questions Regarding the Board of Directors

While some insurers report following certain leading BOD practices, others show insufficient evidence regarding BOD capabilities, time devotion, oversight of management, or independence.

The SQA I submissions are mixed in respect of the BOD. Some insurers show an effort to pursue leading practices, while others come up short on demonstrating that their BOD members have all the necessary capabilities or independence or are attending sufficiently to all their duties.

At some insurers it is less than clear how much and how well the BOD (a) involves itself in critical matters (e.g. setting the company's risk tolerance and appetite, approving any actions that go beyond agreed risk limits, helping resolve risk dilemmas, etc.); (b) takes a lead in ensuring that appropriate control functions are in place and have the right resources; and (c) supervises and challenges management as needed, including in the CG/RM/ICS areas.

Other areas where the SQA I submissions of some insurers suggest lack of clarity or potential weakness in respect of the BOD[4] are:

- Recruitment and selection of BOD members (there is a potential risk to independence if this process is led by management, not the BOD)
- Succession planning for BOD members
- Concrete conflicts of interest policies and compliance processes for BOD members
- On-going training for BOD members
- BOD self-evaluations or external evaluations
- Insufficient prominence of the BOD in setting or being part of the "tone at the top"[5] of the insurer.

At the same time, the SQA I submissions reveal various efforts among Swiss insurers to strengthen BOD governance. These include:

- **Governance Policy.** Some insurers have developed a governance policy for the boards of all their entities, setting out competence, selection, and other criteria which their entities must follow (subject to applicable law). This helps create governance consistency among the boards of all affiliated entities.
- **Use of External Board Members for Subsidiaries.** For parent company boards it is common to have external board members (i.e. independent individuals not employed by the parent or any

[4] The apparent BOD shortcomings at some insurers may be related to various factors, including competencies of BOD members, time devoted to their duties, and different appreciation among them of the nature of their role and duties, whether as mere advisors or also as overseers constituting the most important component of the company's checks-and-balances.

[5] The "tone at the top" refers to the totality of the signals and messages which the leadership of a company sends through their conduct and their communications about what is important at the company. It includes the values, risk appetite, and strategic priorities of the company.

other entity affiliated with the parent). It is less common for subsidiary companies to have external board members. Some Swiss insurers do use external board members for their subsidiaries as these can bring additional perspectives and contribute to independence.

- **Specific Competencies Requirements for Members of BOD Committees.** Some insurers have set out extra qualification requirements for BOD committee membership, such as requiring that a majority of the audit committee members have financing or accounting experience. This is consistent with the Swiss Code of Best Practice and with growing international practice.
- **Minority View Protection.** At least one insurer has in its organizational rules a clause to facilitate the airing of minority views by BOD members. Where a BOD member feels he or she has a major difference with the majority, such member has the option to consult with the BOD Chairman directly. While every BOD member clearly has the right to express his or her view and to discuss matters with the Chairman, the practice here appears to be based on a consideration of group dynamics where perhaps a board member may not feel comfortable under certain circumstances raising certain concerns during the full board meeting. Other insurers specifically note the right of any single BOD member to call a BOD meeting at any time if he or she believes it is necessary.
- **Limitation on Board Mandates.** Several insurers have limited the number of other boards on which their BOD members can serve. One insurer limits this to three. Such limitations can help avoid that a board member is overstretched and unable to devote sufficient time to his or her BOD duties.
- **Consultation with External Experts.** Some insurers underscore in their organizational rules or BOD committee charters the right of the BOD and BOD committees to hire directly and consult external experts to provide them an independent view or advice as they deem necessary. In the area of compensation, for example, this could be very helpful so that BOD members can get the independent view of a compensation expert hired by the BOD, not by management.

5. Increasing Use of Board Committees

There appears to be an increase in the BODs that have committees. An Audit committee is the most common. The governance of BOD committees at some insurers, however, appears suboptimal, with insufficient attention to a committee's mandate and mode of operation.

Checks-and-balances apply not only in respect of the relationship between the BOD and management, but also in the relationships within the BOD. Toward this goal, some insurers set out clear responsibilities for the BOD Chair and other BOD members, and often create BOD committees when the size of their company or BOD makes this sensible. BOD committees not only serve to avoid concentration of power in any one BOD member but can also serve goals of efficiency, quality, and independence. A committee can allow designated BOD members to specialize in a topic, deal with it efficiently, and make more objective recommendations.

The frequent existence of an Audit Committee is to be expected since the Audit committee is a priority in a governance system given its focus, among other things, on the reliability of the financial reporting process. Some mid size and many larger insurers also tend to have a Compensation and/or Nomina-

tions committee. Other types of committees being used by Swiss insurers include Risk, Governance, Investments, and Strategy committees as well as various combinations thereof.

FINMA is aware that the mere existence of a BOD committee does not mean that it is effective. As with overall BOD effectiveness, the effectiveness of a BOD committee is largely dependent on the qualifications of those on it, their leadership, and their spirit of mind to take the committee duties seriously. It is also dependent on how clear the committee's role is and how well structured and run it is.[6]

6. Unclear Checks-and-Balances as Between the Board and Senior Management and Within Senior Management.

As indicated earlier, the SQA I submissions reveal some uncertainties regarding how vigorously the BOD at some insurers are carrying out their checks-and-balances role vis-à-vis management. Where a BOD is not well positioned to carry out this role, it becomes even more important for other parts of the company to be in balance, including management itself.

MB structures

A well-structured MB can be helpful not only to better manage the company but to avoid undue concentration of power in a CEO or any other management member. In their SQA I submissions some Swiss insurers insufficiently document or explain the allocation of responsibilities as between the MB and the CEO. Who does what is sometimes unclear. From the documentation of some insurers it is not evident whether the MB is a decision-making organ that formally votes on key matters or merely an advisory or consultative platform.

While the SQA I submissions show some shortcomings, they also reveal various efforts by insurers to address the CEO/MB checks-and-balances issue. Some examples:

- The CEO must seek the advice of the MB[7] on major matters (i.e. the MB is only consultative not decision making but the CEO must engage the MB).
- The MB is decision making, but can be overruled by the CEO (i.e. veto power).
- The MB is decision making, but can be overruled by the CEO; however, whenever the CEO exercises his veto power, he must notify the Chair of the BOD.

[6] If a BOD chooses to have a committee, it would be expected that (a) the existence of such committee is included in the organizational rules or other similar document of the company and (b) a sufficiently detailed charter or mandate (including rights and responsibilities) exists for that committee (unless the organizational rules already provide sufficient detail). SQA I submissions show that some insurers lack these basic governance documents or that such documents are not of the requisite quality. Sometimes these documents are outdated, unclear or lack details on the responsibilities of the committee or how it is to operate. Good practice examples include insurers who set out in their Audit Committee Charter what the Audit Committee expects in the reports it receives from management and the control functions and what role the Committee plays in any internal investigation at the insurer involving any major violation of law or any allegation against senior managers or persons in control functions.

[7] At some smaller insurers where the CEO is the only member of the MB, he must get the approval of the full BOD or of the Chair for a longer list of things than if there were a multiple-member MB.

- The MB is decision making but in case of a tie, the CEO has two votes. Thus the CEO can break a tie but he can't overrule the MB where the vote difference is more than 1.
- The MB is decision-making, except as to certain specified areas (e.g. certain powers are reserved to the CEO such as hiring personnel below a certain level or approving transactions below a certain amount).
- The MB is decision making and the CEO, like any other member of the MB, only carries one vote.

Who selects MB members? Who decides on MB compensation?

Aside from the structure of the MB, another key indicator of power allocation at an insurer is who can hire and fire MB members and who determines their compensation.[8] SQA I submissions show various practices. Some insurers clearly allocate this responsibility to the BOD or require formal BOD approval. Others appear to have a mixed approach of joint BOD and CEO decision-making, or a split such that the CEO appoints MB members while the BOD determines their compensation or vice-versa. And yet others leave these areas entirely to the CEO (which could create a risk of an MB that is beholden to the CEO and perhaps less willing to challenge when necessary).

MB committees

As in the case of a BOD, a MB can increase its effectiveness and governance through an appropriate use of committees where the size and needs of the company justify this. Such committees can also allow for expert focus on specific subjects. An additional benefit is that they can force the MB to engage itself more deeply in a certain subject and increase thereby MB competence and accountability in this area. The SQA I submissions show some but not extensive use of MB committees. Some of the MB-level committees being used include risk, asset-liability management, strategy, budget, and corporate social responsibility.

7. Among the Control Functions, the Internal Auditor Appears the Most Established.

Based on the SQA I submissions it would appear that the internal auditor and the appointed actuary are more anchored at Swiss insurers than other control functions. The position of the risk officer appears to be gaining increasing acceptance at Swiss insurers but many issues remain (see Observations 8 and 9 below). Other than at certain larger insurers, compliance officers and ICS managers appear the least well established (see Observations 11 and 13 below).[9]

[8] Regarding compensation, see Margin No. 9 of the Circular "Corporate Governance, Risk Management and the Internal Control System for the Insurance Sector" (regarding the use of an appropriate compensation system which promotes the long-term interests of the company and ethical conduct) as well as FINMA Circular 10/1 "Compensation Systems" of November 2009.

[9] Some insurers are also seeking to promote governance in general through various means, including by enhancing the role of the corporate secretary. In such situations the question is the independence of such function and whether it carries out a checks-and-balances role or only a more ministerial role.

Many insurers are able to show through their answers and documentation an internal audit function whose position, reporting (usually to the Chair of the Audit Committee of the BOD), and operation is relatively clear. An annual or multiyear audit plan is often in place and access to the BOD seems unimpeded.[10]

Many insurers are also able to show proper positioning for their appointed actuary. However, some insurers provided insufficient actuary documentation with their SQA I submissions. Also at some insurers there are other issues that cloud the clarity of the actuary's independence or his or her ability to be free from undue influences or distractions, such as when the actuary is too junior or has additional roles. At some insurers where the actuary carries out other roles it is not always clear whether the company recognizes the potential conflicts of interest that could arise or, if so, how it acts to mitigate them.

8. Increasing Evidence of a Risk Manager but Shortcomings Exist.

The SQA I submissions suggest that institutionalization of the risk manager has begun among many medium and larger Swiss insurers. The answers and documentation of these companies show a growing recognition of the role and value of such a function.

Smaller Insurers

Some smaller insurers also exhibit an appreciation for the need for a risk manager but only a minority indicates having a dedicated, distinct risk manager.

With respect to subsidiaries of groups, many indicate having a risk manager but it is not always clear if the risk manager referred to in the SQA I submission is a separate employee of that entity or simply the risk manager of the group. If it is the latter, questions sometimes arise as to whether such person spends sufficient time at the subsidiary in question to properly carry out robust local risk activity.

Governance anchoring of the risk manager

The SQA I documentation of some insurers contain risk manuals that describe risk management activity but do not touch sufficiently on the risk manager's authority and specific responsibilities.[11]

Some insurers do address in their governance documentation (such as in their competence or authority matrix) questions such as:

- When does the risk manager have to be informed in advance of a matter?

[10] Some smaller insurers have been exempted from the requirement of having an internal auditor function on petition to and approval from FINMA.

[11] Moreover, as mentioned under Observation 3 above, only a small minority of insurers have updated their organizational rules or their competence matrix to specifically mention the risk manager and formally set out (as is done for the BOD, the CEO, the MB, and often the auditor) his or her role as part of the company's governance system. When the BD needs to be notified if management is planning changes that may affect the risk management function is also often not addressed.

- When is his or her input required?
- When is his or her concurrence or approval necessary?

Positioning, reporting structure, and independence

The SQA I submissions of some insurers describe a risk management function that appears to have unobstructed access to the BOD. At other insurers periodic reporting by the risk manager to the BOD appears to be well established but it is less clear if the risk manager can discuss with the BOD issues outside of the established reporting plan or without management being present. Also unclear is the extent of any management pre-approval of matters reported by the risk manager to the BOD, a factor that clearly can affect independence.

The level of seniority of risk managers also varies. At some insurers it is a senior-level executive with a rank equivalent to or just below that of a MB member. At other insurers the risk manager's rank is closer to a mid-level or junior manager, something which can adversely affect his ability to prevail on decisions or recommendations. A small number of insurers have made their risk manager a full voting-member of the MB. This is a practice on which there is some debate, such as to whether it enhances the risk manager's effectiveness or whether it can compromise his or her objectivity.

Besides BOD reach and seniority of the risk manager, another critical factor is to whom such person reports as a personnel or administrative matter. Who evaluates the risk manager and who determines his or her bonus or salary increase? What processes are in place for the dismissal or demotion of the risk manager?[12] Based on the SQA I submission a range of practices is evident. For example, some risk managers report to the CEO directly, while others report in to the Chief of Staff, Chief Administrative Officer, Head of Corporate Services or similar.[13] At some insurers the risk manager reports to someone much lower in the organizational structure, which can raise questions about his or her ability to have impact. Questions can also arise when the risk manager reports into someone with direct business operating or financial responsibility (besides the CEO), such as the head of a business unit or the CFO.

Resources

The SQA I submissions raise some questions as to whether appropriate investment in the risk management area is currently being made at some insurers.

Resources for any function, particularly those functions deemed part of the corporate overhead and which do not generate income directly, is of course an issue at most companies. Economic efficiency rightly requires companies to scrutinize and prioritize carefully before adding new functions or new personnel. But resource decisions need to take into account not only immediate budget considerations but also the longer term health of the enterprise. Any underinvestment on CG/RM/ICS now could

[12] A matter for a BOD to determine is the right level of its involvement in the recruitment and dismissal of senior personnel in key control functions.

[13] The BOD should ensure that any such arrangement does not compromise the risk manager's access to the CEO or the BOD and does not result in any filtering of information.

be more costly to an insurer in the future, not only due to the company having to pay later to "catch up" but because of potential problems that can beset the company in the meantime.

9. Insurers' Preparedness in Respect of Their Key Risks Varies Widely.

The SQA I submissions of insurers show a highly mixed picture in respect of activities to identify, assess, report on, monitor and address key risks. Some submissions show considerable sophistication, while others raise doubts on the insurer's ability to reliably recognize if a key risk exists in the first place.

With respect to risk identification, the SQA I submissions show that more insurers are able to identify generic risk areas than those who are able to set out more specific risk exposures based on detailed considerations. If the identified risk area is too broadly defined, determining specific mitigation actions becomes more difficult[14]. Other areas where questions arise are:

- **Effectiveness and timelines of reporting processes for risks** (is reported information useful and up to date? where are the bottlenecks? how is risk, compliance, and other related reporting leveraged?)
- **Risk assessment** (who sits around the table when risk assessments are being done? who challenges if a risk assessment is too optimistic?)
- **Methodologies for risk aggregation and correlation** (are concentration of risks reliably calculated? are smaller individual risks aggregated that separately may not reach a threshold of concern but which together may constitute a material risk? are risks from the various parts and lines of business of the company analyzed for possible correlation and interdependencies?)
- **Risk monitoring** (how are changes in an identified risk monitored and by whom? at what point are such changes reported up for action?)
- **Risk modeling and stress testing** (does the insurer possess sufficient expertise in modeling, scenario planning, and stress testing?)
- **Managing risks** (beyond risk identification, assessment and reporting, how strong are the insurer's capabilities to actively manage those risks?)

10. Less Advanced Practice on Operational Risk

Compared to other risk categories, structured work on operational risk appears less well developed among many insurers.

[14] Another area where a development need may exist at some insurers is emerging risk identification. In this respect relevant questions include: Does the company have a specific process for listing possible future risks and monitoring their development? Does the company sufficiently involve representatives from the various lines of business and the risk engineers to more reliably identify emerging risks among the industries it insures? Does it involve the company's legal department and compliance function to identify future legal and regulatory trends that may come to represent a serious exposure for the company?

In their SQA I submissions some insurers show only a beginning understanding of this topic as a risk category.

Some insurers simply cite the standard definition of operational risk but do not demonstrate the approach the company uses for addressing the various elements of operational risk. The operational tools that many insurers report they use are rather rudimentary such as surveys completed by managers. Relatively few insurers report a robust, systematic approach for identifying, tracking and incorporating operational risk factors into strategic planning, management processes, and decision-making processes.[15]

A connection many insurers fail to make is between operational risk efforts and the company's emerging risk identification processes. Another area of potential weakness among some insurers is business continuity management.[16]

11. Larger Catch-Up Need On the Internal Control System

When RM and ICS (excluding traditional audit activity) are compared, many insurers seem more behind on ICS; the critical element of internal controls over financial processes is not sufficiently demonstrated in some SQA I submissions.

The SQA I submissions suggest that many Swiss insurers are still in the early stages in developing g a comprehensive, coordinated, documented, and actively managed internal control system.

Only a small number of insurers indicate in their SQA I submission having a distinct ICS function or manager (see also Observation 7 above) to oversee the workings of the various controls the company has in place. Some insurers give an insufficient sense of their company's overall control environment or of the kind of specific controls they have at different levels, whether preventive or detective, and who operates or checks these. In their SQA I submissions few insurers show sufficiently how controls are tailored for the size, probability, or complexity of the risk. While some insurers indicate that historically the internal audit has reviewed the existence and effectiveness of specific controls, the nature and intensity of such reviews is not always clearly presented.

The above may have various explanations. The specific requirements in the ICS area—including those relating to the external auditor having to review and report on the existence of a company's ICS under OR 728a and 728b—are recent. Second, there are boundary and definition issues as between risk

[15] The above shortcomings may reflect in part the difficulties in the risk management field in general on how best to approach operational risk, what to include in it, and how to assess it. This may not be an insurer only weakness: a similar weakness is commonplace at many companies in other industries.

[16] Numerous insurers fail to demonstrate in their SQA I submissions that they have a business continuity management program in place or one that adequately covers key areas. Among entities belonging to a group it was common to submit the group's plan which often says little on how the entity at the local level deals with its own endemic issues in case of events that could imperil the company's ongoing local operation. A gap at many insurers is not connecting business continuity efforts to contingency planning for the incapacity or unavailability of key managers. This is not just about succession planning but about planning for what to do if key decision-makers are temporarily not available. The goal is ensuring a company's ongoing operation, even when unexpected events affect those who would otherwise be making decisions when an emergency or catastrophic event arises.

management and internal controls.[17] Lastly, some insurers indicated in their SQA I submissions that they were just beginning their work in this area. It could be that since the SQA submissions many have advanced further in their efforts to develop a systematic and enterprise-wide approach to internal controls, beyond mere periodic audits by the internal auditor.

Controls over financial reporting

One key ICS goal is to provide reasonable assurance on the reliability of a company's financial data and financial reporting. Due to the limited nature of the questions which SQA I asked but also to insufficient explanation by some insurers regarding the scope of their ICS efforts, it is difficult to determine from SQA I alone how rigorously some insurers are subjecting their financial reporting process to robust controls and how well these are integrated in an overall ICS approach. Here the BOD of an insurer, and particularly its Audit Committee, should look carefully at the observations and recommendations of the external and internal auditors regarding the ICS and review regularly the capabilities and performance of their insurer's finance function, including financial controlling and accounting.

12. Uncertainty on Decision-Making Use of Risk Data and Analyses

It is uncertain how much the BOD and MB use for decision making the risk data and analyses they receive from the control functions.

SQA I submissions of many insurers do not sufficiently illustrate the extent to which the various reports and other input and analyses prepared by the risk management or other control functions are used for actual decision making by the company's BOD, MB and other key decision makers.[18]

This is the case even for insurers demonstrating relatively advanced risk analytics and mechanisms for risk reporting in their SQA I submissions. It may be that some decision makers do not give enough weight to risk information from the control functions in forming a view and making a decision. Or it may be that they are not always receiving the right kind of risk information on a timely basis to help make decisions.

The BOD and MB should require adjustments if the risk information being delivered to them is not of sufficient practical value or timely enough for decision-making.

[17] In their answers insurers show different understandings and use of expressions such as "managing a risk" versus "applying a control in respect of a risk". Some appear to see an internal control system as part of a risk management system, while others appear to see it inversely or interchangeably. The more process, assurance, and quality improvement nature of an internal control system does not fully come through in the SQA I answers of many insurers, nor does a connection of their ICS to their compliance and related efforts.

[18] For most insurers, it would be valid to also verify whether employees at all levels, not just BOD members and senior managers, are being sufficiently reached by risk management efforts. Do employees have easy access to the risk management manual and other risk policies? Are the latter written such as to be useful in real-time as employees make decisions daily? Do employees know the insurer's risk appetite and risk limits? Do they know where to get risk management assistance?

13. Insufficient Clarity on Reach and Impact of the Compliance Officer.

Similarly as with the risk manager, the development and acceptance of the position of the compliance officer has begun among some Swiss insurers but appears to have gone less far. At some insurers compliance is recognized more as an activity, rather than as a key function with appropriate strategy, resources, weight, and reach.

Reach and impact of the compliance function

Of those insurers able to demonstrate in their SQA I submissions that they have a compliance function, only a minority describe a function that appears sufficiently well positioned to have meaningful involvement and impact in all key areas. Few submitted evidence of a compliance strategy or a compliance operational plan and even fewer showed how such strategy and plan relate to the company's business strategy and development goals.

The SQA I submissions suggest that at some insurers the compliance function's mandate may be too narrowly defined or it may not be staffed by personnel of sufficient seniority, depth or breadth. At such insurers there tends to be less evidence of such function being able to provide leadership, ensure that identified compliance risks are addressed, and serve as a check on management. At some insurers the compliance function's narrow focus or how it is staffed may prevent it from being involved in certain legal or regulatory areas or in driving company-wide initiatives to increase overall sensitivity to legal and regulatory obligations and sound, ethical decision-making. At such insurers, the compliance function does not seem directly engaged in affecting company culture.

Compliance activity

Some SQA I submissions do not permit determining the extent that appropriate compliance activity is taking place. Some insurers appear to have simply re-labeled their legal department as "legal and compliance" to address the call for compliance but may not have adjusted the activity to focus on things such as compliance processes, training, risk identification, awareness-raising, and compliance controls. Other insurers appear to have added "compliance" as part of the job description of one of the company's in-house lawyers but have not increased such person's authority or positioning.

In all, the SQA I submissions raise the possibility that there may be a general weakness on compliance as a function at a number of insurers. For smaller companies with fewer resources some of this could potentially be made up through creative approaches. For example, a few insurers without a compliance officer indicate having a compliance committee. Such an operational committee can be effective if the various areas of the business are represented in it with the right personnel, if other control functions are members, and if such committee is strong enough to either make decisions or make strong recommendations.[19] Such a committee should be accountable for specific compliance goals, have a charter and otherwise operate consistent with good governance practices.

[19] An operational compliance committee is not to be confused with a BOD compliance committee. The latter is a leading governance practice which can be pursued in addition to having a compliance committee at the operational level.

Resources and independence

As in the case of risk management, success in advancing compliance may also depend on how independently the compliance officer can act and what resources are available to him or her. Since the compliance function's responsibilities include challenging management on proposed actions that could cross onto impermissible areas or that may be legal but not consistent with the company's values, appropriate access to and backing from the BOD also appears critical.

14. Insufficient Internal Compliance Measures

Some insurers show insufficient evidence of specific policies, processes, controls and training on key compliance subjects, including conflicts of interest.

The answers by some insurers reveal potential weaknesses or gaps in a number of key compliance areas.[20] A summary of some general impressions is below:

- **Insufficient sensitivity to conflicts of interest.** While more and more insurers appear to recognize the importance of this area, others appear still to be at an early stage, apparently not having given sufficient study to where conflicts of interest could specifically arise at their company and what to do if they do. Some insurers did not submit a conflicts of interest policy and it is not clear if one exists. Where submitted, the policies are of widely varying quality.[21]
- **Only rudimentary approaches to insider dealing.** Only a few companies appear to have advanced practices in this area, such as having close or quiet periods, keeping insider lists, and specifically having the compliance function clear trading in the company's securities by the company's BOD members and senior managers.[22] Some appear to cover with their insider trading policy an insufficiently small population at their company, focusing only on the MB and BOD, for example, and not recognizing that others at the company could come to be in possession of price-sensitive information.[23]
- **Weaknesses in the means for reporting concerns or violations.** Only very few insurers demonstrate having an operational and well-communicated mechanism for employees to confidentially report compliance, ethical or other concerns or actual violations. Some insurers answer simply that an employee is to report such matters "up the management chain", showing insufficient appreciation of the value of having various means for information to be promptly communicated to

[20] Several SQA I questions requested insurers to describe how they address certain key compliance areas. These include a) conflicts of interest, b) insider trading and c) the means for employees to safely report a concern, lapse or violation. Insurers were also asked if their company had a code of ethics, code of conduct or similar.

[21] Some policies are too short to provide guidance. Others are written more as complex legal documents, rather than as user-friendly compliance tools to help the employee understand his obligations. In some cases, the policies leave unclear who makes a decision if a conflict arises. The scope of the conflicts policies is also often unclear. For example it is unclear at some insurers if the conflicts policy also applies to the BOD members. Some policies show leading practices, such as expressly prohibiting that the same BOD member or manager signs for both parties in an inter-company transaction.

[22] One insurer requires compliance pre-clearing of any trading in securities, from whatever company, by the members of the BOD. Whether this is required also of that company's MB members is not clear.

[23] A few companies indicate not needing to worry about insider trading since they are not a stock-exchange listed company. This fails to recognize that the issue is not just the insurer's own securities but those of other companies in respect of which an employee of the insurer could come to possess price sensitive information in the context of his or job responsibilities.

the right levels of the company, without fear of the information being slowed down, filtered or blocked along the way, or without fear by the reporting employee that his or her employment will be adversely affected.[24] Some insurers provide a confidential channel for communication but limit it for the reporting only of violations. This limits the value as it does not cover more preventive reporting, such as on gaps, weaknesses, or improvement needs.

- **Codes of ethics/conduct do not exist, are at an early stage, or are not strategically connected.** Many insurers have codes of ethics or conduct but some do not. Among those having a code, the quality or coverage is sometimes below par. In some cases a company shows an acceptable code but does not demonstrate how it ties in to the company's core values, strategy, and other platforms that drive the company. The absence of this connection could make the code of conduct less effective.
- **Work appears needed on processes, controls and training.** Some insurers that demonstrate having certain compliance policies and a proper code of conduct often do less well on showing that these policies are accompanied by specific processes for implementing them and by specific controls to determine if the policies are being followed and the processes are effective. Very few insurers sufficiently show that they are specifically linking these areas to their operational risk approach and calculations. Disquieting is the low evidence of reaching out to and training of employees, both on the compliance and the risk sides.

E. Conclusion

The SQA I exercise has been valuable to FINMA in providing it new supervisory insights both on individual insurers as well as on the Swiss insurance market as a whole. These insights will assist FINMA in its efforts toward more risk-based, prioritized supervision.

As with any other first effort, FINMA has identified certain limits and improvement needs in the SQA approach. FINMA will address these in SQA II which when launched (target: 2011) will have increased focus on the effectiveness of a company's CG/RM/ICS strategies and systems, rather than only on their design. Key questions for FINMA will be, how well are these working? What effect are they having on the quality of risk taking and on outcomes? How sustainably are they embedded in company culture and the way the company does business?

The BOD of each insurer should ensure that their company continues to give priority to their efforts in the CG/RM/ICS areas, adjusting and intensifying these efforts where needed. In this connection, it may be of benefit for the BOD, management, and the control functions to review together progress their company has made since its SQA I submission and to design further improvement actions as needed, taking into account any changes to its risk profile, market developments, and relevant lessons from the recent financial crisis.

[24] Some insurers lacking mechanisms for confidential compliance reporting also tend to show weaknesses on processes for employee reporting of risk concerns. If this is the case, it would be most unfortunate if bad news—whether of a regulatory, ethical or risk nature—had no efficient avenue for getting on time to the BOD, MB, risk manager, compliance officer or other responsible organ or person.

Summary of Potential Improvement Areas

Areas where the SQA I submissions reveal insufficient clarity or potential improvement needs at some insurers include:

- Board of Directors' capabilities, time devotion, oversight of management, and independence
- Checks-and-balances as between the BOD and the Management Board within the MB
- the positioning, resources, independence, reach and authority of some control functions
- company preparedness overall to manage risks effectively and comply with obligations, including in terms of having in place necessary policies, processes, training and controls.