

A. Thomas Finnell, Jr., CPA

January 18, 2005

To: Leslie Geel, by e-mail: lgeel@naic.org
Annette Knief, by e-mail: aknief@naic.org
National Association of Insurance Commissioners

Comments on Risk Assessment Working Group's Proposed Revisions to the Examiners Handbook

Ms. Geel and Ms. Knief:

I am pleased to submit the following comments on the Risk Assessment Working Group's proposed revisions to the Financial Condition Examiners Handbook. These comments are submitted on my own behalf, and are based on my past experience and involvement in various examinations, including efforts over many years to assist states in implementing examination protocols that are responsive to the unique profile of each insurer.

As you well know, the proposed changes to the handbook are extensive. In the time that was available to me, I have tried to capture some of my thoughts in writing about a number of the proposed changes, not to serve as my final words on the matter, but rather as a starting point for dialogue with you, the RAWG, and other interested parties. I hope that working together, we can all better understand the potential implications of what is being proposed and suggest further changes as necessary to arrive at an approach that is theoretically sound, practical to implement, and cost-beneficial.

I hope that you will find these comments constructive and helpful as you strive to improve upon the handbook.

Sincerely,



A. Thomas Finnell, Jr.

Risk Assessment: A Vision

Changes to the Examiners Handbook should better enable regulators to view a company and its risks from a perspective that is not unlike that of management. Regulators would still form their own assessment of the company, but having a platform from which to view the company that has more in common with that of management should enable a better focus by both parties on issues of risk that matter.

Traditionally, regulators, insurers, and independent auditors took considerably different approaches to their work which, of course, is not surprising in light of their very different roles and responsibilities. Management developed and relied on procedures and controls to record transactions and to establish balances for financial reporting, in some cases subjecting them to internal audit or other quality control testing. The company's independent auditor might have reviewed and tested those controls, but often would not, citing efficiencies through substantive procedures. And state insurance examiners would typically perform their own procedures, which too often would not necessarily be correlated to the company's procedures or controls, or to the tests performed by the independent auditor.

Each party drew their own conclusion about the presentation of the financial statements. Nonetheless, and despite their mutual need to better understand risk, their separate processes were not aligned so as to maximize the attainment and sharing of risk-related information that would be relevant to each other, much less to enable a meaningful dialogue to evaluate the significance of that information and its potential implications to the company. In that respect, the management-auditor-regulator triumvirate was marginalized with respect to their collective abilities to address risk.

My point of view is that the confluence of two events will go a long way toward rectifying that situation. First is the Sarbanes Oxley Act of 2002 (SOA) which, among other matters, requires a higher degree of diligence for management and boards of public companies with respect to governance and financial reporting. Furthermore, and with the new requirements of the SOA-inspired Public Companies Accounting Oversight Board, independent auditors are now required to perform integrated audits, reporting separately on the company's financial statements and on its internal controls. No longer can auditors perform substantive procedures in key areas in lieu of evaluating a company's internal controls. In these and other ways, the SOA addresses certain of the risk-related contributions from two out of three members of the aforementioned triumvirate.

The second event will address the third member of the triumvirate, insurance regulators. Specifically, the prospective adoption by the NAIC and the implementation by state insurance regulators of a risk-based surveillance and examination approach that considers and leverages the work being done by management and its auditor, contributing to the equation the regulator's perspective about risks, while minimizing the duplication of effort, disruption to the company, and unnecessary costs.

It is that vision that draws my support for the RAWG's objectives. However, I have various concerns and suggestions for consideration by the working group, which are described below.

Comparison to the SRA Approach:

The Specific Risk Analysis (SRA) approach was originally developed by a large accounting firm as its internal auditing methodology. The methodology had been used provided in conjunction with an examination-related project on behalf of a state insurance department, who in turn provided it to the NAIC for consideration at a national level. After much discussion and some refinements, it was adopted into the Examiners Handbook, and later became part of the Financial Regulation and Accreditation Standards. Notable about the SRA approach is that:

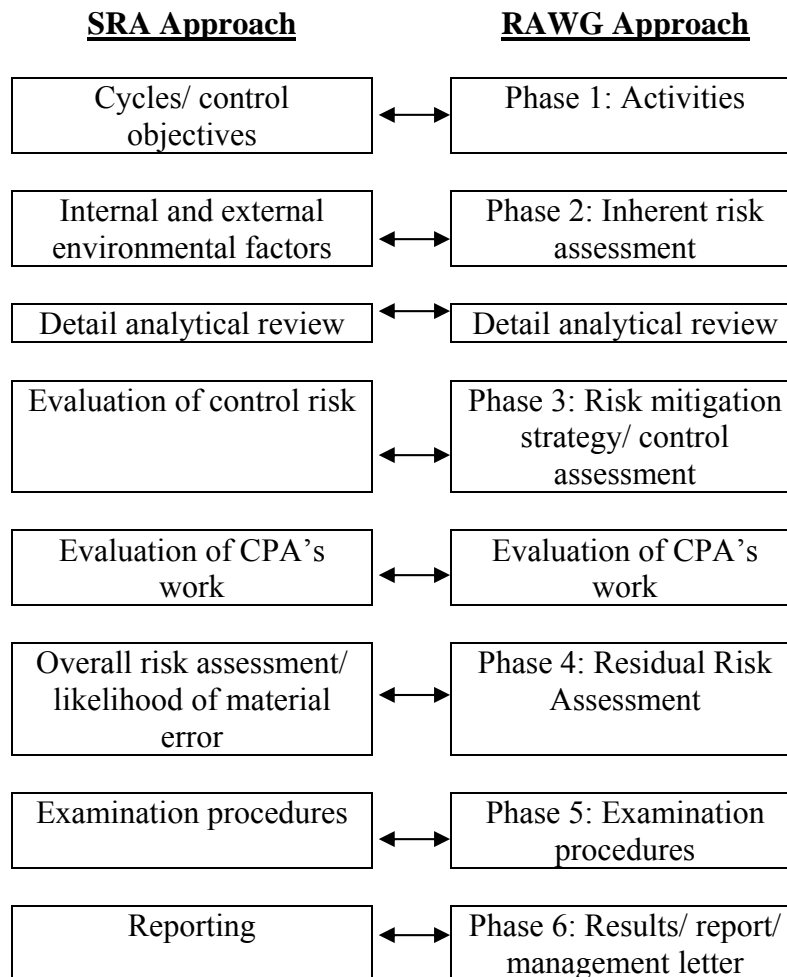
- It is a risk-based approach, albeit one that is focused on financial reporting and those risks that relate to amounts or disclosures that are reported currently in the financial statements.
- There appears to be a widely-held view, including by the RAWG, that the SRA-based approach is not being followed in practice. In other words, examiners are not sufficiently modifying procedures to be responsive to risk, rather, they have been more apt to use a more standardized list of procedures from one exam to the next.

In turn, that leads to the following conclusions:

- Other risks that may manifest themselves in the form of losses/liabilities after the current financial reporting cycle are not necessarily covered in the current SRA-based approach, and it would be fruitful to assess those risks as part of the RAWG's proposed examination process.
- There is something very wrong with the deployment and execution of the current approach. Whatever that is, it has been ongoing for over a decade. There also is the very real risk of replicating that problem as the NAIC moves toward finalization and deployment of the RAWG's proposals.

The former may be addressed through revisions to the approach itself. The latter may be so addressed as well, to the extent that a well-written and easily understood handbook contributes to the process. However, there are other aspects of deployment, including a roll-out strategy, training, and ongoing monitoring that also must come into play. More thoughts about the proposed handbook language and deployment are included later.

It is instructive to compare the key aspects of the SRA methodology to that currently proposed by the RAWG, as embodied in the Risk Assessment Matrix. That is not to suggest in any way that we should be wedded to the past, rather, a conscious comparative exercise is simply useful as a framework to extract some observations for consideration. The following chart strives to match the key aspects of each approach for comparison purposes, with discussion around key points following the chart:



Cycles/Control Objectives v. Activities:

The SRA is simply a tool that self-contains a structured methodology, together with some pre-populated content (cycles and control objectives) that enable exam teams to approach any insurer with some degree of uniformity while at the same time tailoring the approach to the unique facts and circumstances at the company under exam. The use of cycles and control objectives tend to self-define, or frame, the scope of the project. Defined at a high enough level, those same cycles and control objectives can apply to most insurers. Thus, from a project management perspective, and with the outside borders of the task now framed it is a matter of working from the outside in to obtain the necessary level of detail

to complete the SRA with respect to material areas, and then determine the examination approach. In other words, there is a finite amount of content that is needed for the examiner to obtain at which point the process is complete.

Under the RAWG's methodology, the organizational units around which the exam will be based are "key functional activities". However, there appears to be no comparable structure to suggest what such activities might be, even in the generic sense. It appears that the list of activities would be built from the inside out, i.e., they would continue to be identified and listed until at some point the examiner concludes that the list is complete. However, going in this direction it would not be clear when "enough is enough." The following additional concerns are presented:

- The term "key functional activities" does not appear to be adequately defined or illustrated. Based on the verbiage used, "key functional activities" might be business activities, and/or risks/events, and/or cycles, and/or processes. This can present much confusion, and also suggests a potentially long and overlapping list of "key functional activities" to be investigated and documented.
- The notion that functional activities would be determined consistent with the company's organization makes sense. However, many public companies that have gone through the SOA internal control documentation, testing and reporting process, have identified large numbers of business processes, reportedly in excess of 1,000 for some. Gleaning information from that body of knowledge for the regulatory exam process will be an arduous, time-consuming, and potentially expensive process.
- For those non-public companies that have not been through that exercise or have not otherwise adopted COSO or another comprehensive internal control assessment methodology, it will be extremely difficult for this type of information to be assembled as part of an exam process that is not somehow linked to an existing company-based process that generates and maintains such information.

Some suggestions are as follows:

- Construct the framework using an outside-in vs. inside out approach. Start with the 9 risk categories to "box in" or frame the project, identify if significant inherent risks appear to exist in each category, and for those, identify only the key business processes that mitigate that risk. For example: Credit risk → investment impairment subrisk → investment valuation process.
- Define "key." Depending on a company's investment portfolio, investment impairment risk may not be significant, and its investment valuation process therefore may not be "key". Alternatively, it may be "key" for only a specific subset of the portfolio.
- In identifying subrisks, it may be helpful for the examiner to refer to the work product that was produced by another NAIC working group that

compared such subrisk categories to those developed by the Federal Reserve Board.

- Examiners should be cognizant of the relative degree of uniformity that exists across the enterprise with regard to a given process. This is especially important for group exams, for which common management, systems, and processes may be in place for certain key areas. Also, risk management will most likely be accomplished at the enterprise v. the legal entity level, which is why the risk assessment approach is most appropriate for exams performed on a group basis.
- Instead of the term “risk”, you may want to consider the term “event.” This is just one way where the approach could be made to be more consistent with COSO’s Enterprise Risk Management Integrated Framework (COSO ERM Framework), which may enable examiners and those in industry to better communicate and understand each other when discussing risk.

Environmental Factors v. Inherent Risk Assessment:

Under the SRA approach, inherent risk was addressed through the consideration of internal and external environmental factors. For example, an examiner would consider that the impact of current economic trends (impact of interest rates on investment valuations) and the sufficiency of management resources to address potential impacts. However, examiners were not asked to specifically quantify that inherent risk under the SRA approach. Instead, an overall rating, known as the “likelihood of material error” was made that considered all the inputs to the SRA: inherent risk, analytical review, control risk, and the work of the CPA.

The RAWG has proposed to include the examiner’s assessment of inherent risk in the Risk Assessment Matrix. Inherent risk would be assessed as to probability of occurrence, potential magnitude, and on an overall basis. This appears to be consistent with emerging practices, and with the COSO ERM Framework. Nonetheless, there are some concerns:

- The nature of information that will be available at the company to help the examiner will vary greatly. The vast majority of insurers have not adopted an ERM model. To a large degree, risk management is a bifurcated process, managed at the operational level with widely varying efforts applied from company to company, and from one risk category to the next.
- For operational risk, for example, it is very likely that the company will not have a comprehensive risk management program in place. Some may view their SOA efforts as a step ahead in handling operational risk, but unless companies have voluntarily expanded their efforts to also cover regulatory and operational risks in addition to financial risks, there will be potentially large gaps. In other words, the company itself, much less the examiner, may not be able to assess impact or probability other than in some broad, anecdotal manner. That means that for non-traditional risks, there is a higher degree of examination risk, i.e., that those assessments will be incorrect and the resulting allocation of examination

resources and focus may not be optimized. In the past, that risk was unconsciously accepted, to the extent that it simply was not covered by the scope of examination. Under the RAWG's approach, that will no longer be the case, and examiners will have to learn to recognize and accept a higher degree of examination risk relative to non-traditional risk areas. In my view, examiners tend to be more risk-averse; yet expanding examination procedures may yield rapidly diminishing returns in terms of mitigating levels of examination risk in the nontraditional risk areas. Consequently, more guidance may be needed for examiners in this area.

- In the absence of any consideration of mitigating controls, most inherent risks may seem significant, the point being that it will be difficult to use the inherent risk assessment to differentiate one area from another for purposes of allocating examination resources or attention. It is easy to foresee much confusion when trying to quantify impact or probability at the inherent level. Even companies that are ahead of the curve in adopting risk management practices may not be able to provide an estimate of probability and impact in a manner that is consistent with how the examiner has identified the "key functional activities."

Some suggestions are as follows:

- Expect a wide degree of variability between risk categories as to the nature and extent of information that will be available, the measures that may be feasible as to probability and potential impact, and the degree of objectivity/subjectivity around those measures. The exam model should be flexible enough to enable examiners to react to these varying circumstances, perhaps including examples of proposed examination responses where a sophisticated risk management model is in place, compared with a situation where a much more unsophisticated approach is in use.
- Provide robust examples of examination responses for categories such as operational risk, where the assessment ranges from low to high. In the short term, this would greatly assist regulators and interested parties alike in better understanding the implications of what is being proposed. In the long term, it will better assure that there is a higher degree of uniformity in implementation across examinations and states.

Analytical Review:

In the SRA model, analytical review is used on an overall level in the initial planning stage, at the account level in preparing individual SRAs, and in some cases as a direct test of balances, i.e., as an exam procedure resulting from the SRA.

In the RAWG's proposed model, each of the foregoing applications of analytical review appear to be retained, with the revision to refer to the risk assessment rather than the SRA. However, the tool that captures the risk assessment, the Risk Assessment Matrix, does not contain a field to capture information from the use of analytical review procedures. Therefore, it appears that analytical review is a potentially important input to

the risk assessment, but one that would not necessarily be considered together with other inputs relative to a particular activity or risk.

Some suggestions are:

- Provide a means to capture key conclusions from the detailed analytical review in the Risk Assessment Matrix.
- Provide guidance to highlight that the analytical review guidance that has been carried forward from the existing Examiners Handbook may be of limited help when assessing non-traditional risks, e.g., strategic, operational, etc.
- Emphasize that in the case of many companies, particularly large, publicly-traded companies, examiners may quickly benefit from the work of external industry analysts' reports, rather than creating their own analyses from scratch.

Evaluation of Control Risk v. Risk Mitigation Strategy/Control Assessment:

In the SRA model, the original intent was that examiners identify the key controls in place with regard to a particular cycle/control objective. Over the years, that has morphed somewhat in that an appendix that had listed typical controls to consider had been pulled forward into the body of the SRA itself. As a result, examiners then too often aimed to use that as a checklist, identifying if an insurer had all of those controls, regardless of their priority or importance in terms of mitigating the underlying risk.

The RAWG's proposal has again relegated the listing of typical controls to an appendix, which should be helpful. However, there are other concerns:

- The guidance should be clear to ask only for "key" controls, and that should be defined, e.g., those procedures that, if executed as designed, would be effective in mitigating risk to an acceptable level.
- The guidance indicates that controls should be tested. For public companies that have been through the SOA internal control documentation/testing/reporting exercise, it would seem reasonable to provide more examination "credit" for that testing.
- The proposed guidance for Phase 3 includes five factors to consider in assigning an overall rating. These five factors appear to be quite broad in application ("manage all the risks in its significant business activities..."). However, in comparing this to the Risk Assessment Matrix, it would appear that the matrix would call for a more specific assessment as to the specific control listed. It would be helpful for the RAWG to clarify their intent with respect to this rating.
- Phase 3 also includes detailed language on management competence, management performance evaluation, board of directors, organizational structure, etc. It is unclear as to why these items of enterprise-wide significance are included in this phase, when examiners are going through the risk assessment process at the "key functional activity" level.
- Phase 3 includes a section on internal control and compliance testing which states, in part, that "controls should be identified and tested after the examiner's

assessment of inherent risk, but before residual risk is determined and significant examination fieldwork begins.” Taken literally, this suggests that there now will be two phases of field work: one for compliance testing, and a latter phase for other substantive tests. In most cases, that would be unnecessary, would extend the timeframe to complete the exam, and add costs without any corresponding benefit. Assuming that an upfront evaluation of the control environment has concluded with a satisfactory rating, it is reasonable for the examiner to proceed in determining the overall examination plan and in executing that plan which would include an appropriate selection of compliance and substantive tests. In rare cases, control testing may indicate that the examiner’s initial planning assessment was incorrect and may cause the examiner to recraft different and/or additional procedures. But in the vast majority of cases that will not occur, at least to the extent that significant scope changes are required. Holding all exams and all areas on those exams to this “two-step” field work process would not appear to be necessary or desirable. Examiners routinely perform procedures with the expectation of finding no problems, adjusting procedures when exceptions arise. There appears to be no apparent reason as to why that should now change.

- That same section describes that a “low or medium risk company may warrant a reduction in substantive testing.” This relates to the nature and extent of examination procedures, should be expanded upon, and would appear to be better placed in Phase 5.

Evaluation of CPA’s Work:

Both the SRA and the RAWG-produced model consider the work of the CPA. Concerns and suggestions regarding the proposed text pertaining to the consideration of the internal audit function and of the work performed by independent auditors are as follows:

- On page 9 of the first section of the text, the statements are made that, “if the scope, quality and oversight of the audit function is adequate, then verification of the full balance sheet may not be a primary examination objective issue. The examination effort could then focus on identifying those risk areas that could lead to deterioration of profitability in the future, potential economic loss and /or solvency concerns.” I agree with those statements, and believe that this would be a substantial change to the way that many exams are now carried out. The concern is that these two sentences will be overshadowed by so much other language in the text, including that in the separate section related to the work of the CPA, that these thoughts will essentially be lost.
- Although references in the text have now been made to SOA and the changes that has caused to the scope of the CPAs work and how it may help the examiner, more thought could be given to the implications of those changes to the regulatory examination process. Pre-SOA, the use of the work of the CPA was analogous to the AICPA’s auditing standard regarding the CPA’s use of the work of the internal auditor, i.e., evaluate the CPA’s capabilities and independence, and make appropriate tests of their work on which reliance is to be taken. Post-SOA, restrictions on non-audit services, combined with the monitoring, investigative

and disciplinary capabilities of the PCAOB, have “raised the bar” (as stated in the RAWG’s proposed text) in terms of the diligence with which independent auditors perform their audit work. Therefore, and all things being equal, it would seem that the need to test that work, or at least as much of it, would be less now than it was back in the early 1990s when the current Examiners Handbook language was first adopted. Ideally, to the extent that a CPA performed a procedure and documented it, there should be little concern. Rather, the main concern has been, and continues to be, simply understanding how the CPA perceived risk, how that risk was addressed and through what procedures, and the judgments that were made along the way. Knowing that, the examiner can then determine whether the CPA’s work affords the examiner some comfort and to what degree. The regulatory examiner can then be in the position to “backfill”, most likely in a small number of areas and/or to an incremental extent, to perform such procedures as are necessary to increase his or her comfort level to the necessary level.

- It is also quite difficult to obtain the necessary understanding of the CPA’s risk and perception of risk by reviewing documents alone. Although there is language in the text suggesting a dialogue with the CPA, in my experience this is only a perfunctory meeting or two, with the main focus being on access to working papers. In fact, this seems to have become largely a compliance exercise. For larger companies, and particularly now for public companies that have completed the SOA-mandated internal control documentation, testing, and reporting, it will likely be necessary to have an overall walkthrough of the work performed by the CPA, first from a macro perspective, and a more detailed walk-through subsequently with regard to specific key areas. The documentation that has been gathered, created and organized by companies, their consultants, and their auditors in response to SOA is both complex and extensive. The proposed language appears to do little to prepare examiners for what they will encounter.
- Regarding the text that describes the differing objectives of examiners and CPAs, and the similarities and opportunities for efficiencies, I would refer you to my opening comments at the beginning of this attachment. I do believe that there is the potential for much commonality of interest between management, the CPA, and the regulator/examiner. If you agree, those same thoughts that I have shared at the outset could be useful in this section, while some of the existing language could be changed. Having said that, it is also important to highlight that the CPA’s SOA-related work is focused on GAAP reporting and will therefore cover only a subset of the risks with which the RAWG is now concerned; that many company systems are used to support both GAAP and SAP reporting but there are some that may remain untested by SOA (e.g., SAP life reserve valuation systems); and that materiality levels used by CPAs for SOA-related testing are defined by GAAP amounts at the SEC registrant level.
- Although there are many implications to public companies that have become subject to SOA, other non-public companies may have undergone similar efforts to document, test, and report on their internal controls. Reasons that some non-public companies are doing so include that they perceive SOA requirements to be

- a best practice, that their business partners (many of whom may be public) expect similar diligence from those with whom they do business, etc.
- Some references appear in need of updating, e.g., with regard to public companies, reference should be made to auditing standards established by the Public Companies Accounting Standards Board.

Other Comments

Deployment

Deployment is certainly an issue with which the RAWG has shown concern, and for good reason. The current version of the handbook was deployed in the early 1990s, and borrowed heavily from the technical expertise, writing skills, and prior deployment experience of one of the large accounting firms across its extensive client base representing various industries and segments. Notwithstanding that apparent advantage, it took years for it to be rolled out to all the states, and many would say that to this day, it is not being used as intended as a risk-based approach.

The proposed changes developed by the RAWG suffer in some respects by comparison to the early-1990s launch of the current SRA-based exam approach: the text borrows from many different sources, mixes traditional concepts (e.g., PM/TE) with newer risk management concepts, has only now been assembled in a comprehensive fashion for review, has no content to illustrate the new Risk Assessment Matrix, and may not have actually been used as a comprehensive approach on any exam to date (or if any, probably very few).

On a more cosmetic level, and like any technical manual, the text is by no means an “easy read.” It is text-intensive, appears to be repetitive about some points, and appears to draw on different sources without sufficient editing to blend styles. Also, there are a large number of exhibits, and from the standpoint of readability, it would be beneficial to take a hard look at those to determine if there is a consistent and easily understood approach to them, i.e., can they stand on their own without a lot of accompanying explanatory text up front, should some of them be collapsed into the body of the text rather than retained as an exhibit, etc.

It is not my intent to be overly critical of the RAWG’s efforts. I believe those efforts are well-intentioned, and from a technical perspective, are directionally appropriate. However, from a project management perspective, examiners will need a reference source that is clear and concise. While the NAIC intends to supplement the RAWG’s efforts with training, it has been my experience that attendees at any training exercise will only retain a small fraction of what they learn. The most practical outcome will be that they will have an appreciation for the new approach, and retain a general awareness of what is in the handbook. But when they actually get in the field, the handbook will be their crutch, and if it is not written clearly and succinctly, it will make their job harder, and result in wide variations in practice. In the absence of clarity, they will most likely fall back on tried and true procedures, and the RAWG’s objectives will not be achieved.

That is essentially what happened in the early 1990s, and the NAIC and the states run the risk of repeating history.

Methodology

I subscribe to the premise that risk management, like financial reporting itself, is first and foremost the responsibility of management and the Board of Directors. As an auditor, or as a regulator, it is useful to understand what management and the Board has done to accomplish its objectives and responsibilities in those very important areas. In fact, it would prove very difficult, if not impossible, to assess a company's financial statements without starting with an adequate understanding as to how the company has approached the financial information gathering, analysis, and reporting processes. Risk management is no different, and also requires at least a basic understanding of the company's approach.

Given that context, it would appear helpful if the Examiners Handbook could first set forth for the benefit of examiners what risk management is from the company perspective. Instead, the text appears to take the perspective of "here is what you as an examiner should do to assess risk at the company under examination." This point can be seen from the chart on page 11 that summarizes the 7-phase regulatory risk assessment process. It would be helpful to instead first depict a typical company's underlying risk management process and then overlay the regulatory approach on top of that to better illustrate how the regulatory approach can benefit from managerial information and to avoid duplication. In that regard, the COSO ERM Framework includes a cube-like diagram illustrating such a model that may be a useful starting point for this purpose, while at the same time emphasizing that the vast majority of insurers do not have a comprehensive, enterprise-wide risk management framework in place.

The text does not appear to adequately address the very different outcomes that can occur across risk categories. For the so-called "traditional risks", those that are most easily related to a balance sheet category (credit risk, market risk, reserving risk, etc.) there will be ample (and perhaps overwhelming) information and documentation as to the company's procedures and controls, information suitable for analytical review, internal and independent audit work, etc. In most cases, the exact opposite will be true for the "non-traditional" risks, those that don't relate to a balance sheet item (e.g., operational risk, strategic risk, etc). The former most easily give rise to traditional examination procedures (confirm, recalculate, etc.). The latter do not. In many cases, inquiries into non-traditional risk areas will yield good information that may give rise to a future "to do" (e.g., follow up in 6 months to determine if there is evidence that the company's new distribution strategy is helping to stave off an otherwise shrinking market share). Both make good information in the context of the overall risk assessment framework. However, the handbook does not adequately describe this phenomenon and how examiners should deal with it.

Other comments include:

- Little is said in the text about other procedures that are intended to determine compliance with state laws (e.g., re: investment limitations) or to gather historical information for reporting purposes (the forepart of the report). For both, the concept of materiality would appear not to apply, but it is unclear if the RAWG wishes to confirm or change that.
- In my experience, the risk-based intentions of the current handbook have too often been disarmed by the belief of many examiners that certain specific examination procedures simply must be done, regardless of the company or its risk profile. In some cases, this is a department-wide rule, in others it is just a personal preference of the individual examiner. It is not clear as to how the NAIC and the states will assure that this phenomenon will not disrupt attainment of the RAWG's objectives.
- The Financial Regulation Standards and Accreditation Program has some important implications to the risk-based approach, as well. The RAWG has mentioned the need to consider the timing of changes to the standards to effectuate the risk assessment process. But a more subtle aspect should also be considered. Examiners currently have little or no positive incentives to be innovative or forward-looking in their thinking when it comes to examinations. On the other hand, they do perceive very negative potential consequences if for some reason an exam "goes bad" or if the state's accredited status is somehow called into question because of findings of accreditation reviewers. In my experience, this has contributed in part to a bias towards examiners using a more standardized and extensive set of procedures and the failure of the existing SRA approach.
- The Risk Assessment Matrix tool appears to be thoughtfully devised, however it is unclear at this stage if it will in fact be helpful on all exams. On larger, more sophisticated companies, it may prove better to focus on what the company has done to document and assess its risks, perhaps mapping what they have done to your regulatory objectives. I would not suggest that examiners "should" use any particular tool, until there is ample experience to support that.
- The 7-step risk assessment process appears to be logically sequenced, however the handbook describes a sequencing of steps within phases that may be unnecessary and lead to inefficiencies. On many exams, there are various aspects that can and probably should proceed simultaneously, rather than sequentially. In a small number of those cases, findings may arise that will require the exam team to reconsider procedures already performed and make adjustments, an inefficiency that could have been avoided had a sequential process been followed. However, that would likely only occur in a minor number of situations, and the benefits of allowing examiners the flexibility to proceed down multiple paths will likely far outweigh, in the aggregate, the additional costs in those few situations.
- The text should give greater emphasis to the use of external analysts' reports in situations where they are available. External industry analysts, on the credit and equity side, are proficient at analytical review, have access to management to make inquiries to supplement their quantitative analysis, and are experienced in translating what they have seen and heard into findings that highlight a company's

risks, its strengths and opportunities, and how it measures up competitively. For public companies in particular where a number of such reports would be available, review of such reports, supplemented with NAIC-prepared benchmarking, may be all that is needed from an analytical review perspective in the planning stage.

- There is language in the text that is helpful in pointing out documents that would be available to the company that would provide various types of information. However, the text should also highlight the key sources of information that should receive primary attention and that would be helpful in getting the exam team up to speed in developing a preliminary point of view about the company and its risks in order to prepare to engage management in dialogues. In my experience, too many examiners appear to be uncomfortable in dialogues with management, other than about perfunctory issues or data requests. The proposed risk assessment process will only heighten those discomfort levels because examiners will be required to exchange thoughts about risk concepts about which they may have little background, and to have those dialogues with higher levels of company management. It would be helpful to point examiners towards the priority sources of information that can help to bring them up to speed and to dispel some of that discomfort, and promote a more meaningful dialogue about risks that matter.

Planning Materiality /Tolerable Error

- It is unclear how the traditional exam concepts of PM and TE should be used going forward in the proposed risk-based approach. The guidance in the current handbook, which is anchored in an approach used by a large accounting firm over 15 years ago, was developed focusing on an audit of financial statements and the need to obtain adequate coverage across accounts and through account-based testing strategies so as to be assured that any material errors were identified and that, on an overall basis, there was a high degree of confidence that the financial statements fairly presented the financial position, results of operations, etc. The proposed text appears to now leverage the traditional concept of PM/TE into additional measurements of inherent and residual risk, not just for traditional balance sheet-related risks, but also for non-traditional risks such as strategic, reputational, operational, etc. For example, the text states, “the materiality of levels set during the planning phase [presumed to be PM/TE] should be used to assess the magnitude of impact.” It is unclear as to how appropriate that would be. Instead of comparing a calculated PM amount to a hard dollar account balance, it would appear that examiners will now be asked to compare PM to a more amorphous figure, that being the potential impact, which for non-traditional risks may not be measured at all by the company, and certainly would not be found in any general ledger account. At a typical 10% of surplus level for PM, one could argue that in many situations, non-traditional risk levels would be deemed material on an inherent basis, and very possibly on a residual basis as well. Therefore, using PM defined in the traditional setting may not sufficiently differentiate risk levels for purposes of allocating exam resources from one company to the next, or by area within a company.

Group exams

- The NAIC is involved in other activities calling for more exams to be performed on a group basis and establishing protocols for state communications and interactions on group exams. I believe that more guidance is needed in the handbook describing the technical aspects of a group exam. Examiners would need to identify which of the “key functional activities” are managed across which legal entities and business units. Doing so may produce significant efficiencies for those groups that are managed with a high degree of commonality among group members as to systems, management, and controls.
- Risk management will most likely be accomplished at the enterprise v. the legal entity level, which is why the risk assessment approach is most appropriate for exams performed on a group basis.

Risk Assessment Tool

- In many public company situations, and as described above, there will be an extensive amount of documentation around internal controls and company and CPA testing of those controls. It will be an arduous task to repopulate content from the company’s SOA repositories into the examiner’s Risk Assessment Matrix. A more practical solution may be to gain an understanding of the SOA-related documentation that the company has prepared, and at a high level to map from that to the examination objectives. Then, on an account or risk-level basis, selected documentation can be obtained from the company, reviewed, and if necessary, tested.
- It would be helpful if the Risk Assessment Matrix included in the handbook could be pre-populated with realistic data to demonstrate, by example, the level of detail that the RAWG believes to be appropriate.

Conclusion

Despite the length of this letter, I believe that the RAWG’s objectives are directionally appropriate. The work product, however, requires more study. The evidence before us suggests that the deployment of the current handbook failed in some respects, particularly about getting examiners to be more responsive to risk. It is therefore incumbent on all to strive to not only develop a sound methodology, but to take those extra steps necessary to assure that this time, the new methodology will be rolled out and implemented as intended.

My recommendations to the RAWG are as follows:

- Slow down and do this as right as you can. The current handbook, for better or worse, served the industry for over 10 years. We are again looking at another long-lived resource, and if it is poorly understood in the field, you run the risk of additional and unnecessary exam costs and higher examination risks across many companies and over a long period of time.

- At the same time that we are evaluating the RAWG's efforts, public companies are about to issue their first internal control reports under SOA. SOA will clearly have some pervasive impacts on the tone at the top within public companies over financial reporting. We should allow some time for the experience of public companies with SOA to emerge to determine the potential implications from an exam perspective before mandating exam methodology changes across the board.
- Develop a rollout strategy that goes well beyond the notion of additional training, such as:
 - Revise the handbook after adequate time to consider comments from regulators and interested parties
 - Release in a "pilot mode"
 - Strategically identify a number of examinations to use the approach in the upcoming exam cycle, covering large and small companies, public and non-public, group and non-group exams, centralized and decentralized companies, different industry segments, etc. – no more than 10 to 20 in total. It would be good to have management of those companies agree to voluntarily participate, not only by allowing a pilot approach be applied to their company, but also to provide feedback from their perspective as to the apparent costs and benefits of the exam approach.
 - Exempt those pilot exams from the existing accreditation standards so that examiners will be free to explore and innovate.
 - Require the pilot exam teams to develop benchmarks that can be used to measure the effectiveness and efficiency of the new approach. They should be required to identify past exam times and costs, develop budgets, and monitor and report on progress. Other qualitative measures could include the number, nature, or dollar value of exam findings, management's perception of the value-add provided by the new approach, etc.
 - Determine that staffing on those exam teams is adequate, and includes one representative (presumably the EIC) who is qualified and able to participate in a peer network in periodic meetings and calls over the next 12 months. While maintaining the confidentiality of company-specific information, the network would share ideas, knowledge, best exam practices, problems, etc.
 - Arrange for the company representatives to also participate in a peer network for purposes of developing some consensus as to the perceived benefits and cost, what appears to be working or not from their perspective, etc.
 - NAIC representatives on the networks would capture those thoughts and the RAWG would use the knowledge gained to consider further changes to the handbook.
 - Once those changes have been made and vetted with industry and interested party feedback, expand the number and scope of exams to be

performed in ensuing exam cycles, with the objective of attaining 100% participation within a certain time frame (e.g., perhaps 5 years).

- Until more experience is gained, tread lightly on risk areas that go beyond financial reporting. The SOA's requirements do not extend to controls around operations and regulatory compliance, and CPAs don't have any mandated involvement in those areas either. So as compared to the current SRA approach, when regulators adopted a proven approach that was in use by CPAs, regulators will now be covering some uncharted territory. Learn what you can and gain some experience before adopting further requirements, the implications of which today can only be conjecture.