

# Examiner<sup>®</sup>

Volume 35  
Number 1

Spring 2010



Official Publication of the Society of Financial Examiners<sup>®</sup>



# HOW TO ADDRESS THE RISKS IN RISK-BASED AUDITS

## AN EXTERNAL AND INTERNAL AUDIT APPROACH

**Lewis D. Bivona, Jr., CPA, AFE,  
Principal and Insurance Group  
Leader for WithumSmith+Brown.**

**Contributing Author  
acknowledgement: Elaine  
Nissley, MBA, CISA, PMP, CCSA,  
Sr. Consulting Manager, Risk  
Management Services Group,  
McKonly & Asbury LLP**

### *Editor's Introduction*

*Just as examiners are adjusting to new methods and processes to meet the objectives of the new risk-based audit approach; by direct correlation, the management of the insurance companies also have to adapt to new demands and requirements placed on them by examiners. Written from an internal management perspective, this article gives useful insight into the challenges and issues now being faced by the management of insurance companies. Additionally, this article provides excellent informational material, which can be passed along to client insurance companies that have questions about the new risk-based approach.*

To paraphrase Tom Cruise in the movie *Risky Business*, "Internal Control, there is no substitute!" Insurance is a risky business, the Fed's say so, the NAIC says so, and even the President of the United States says so. So it should be no surprise to those in the industry that more attention than ever is being focused on inherent entity risk before auditing "the numbers".

In early 2007, Mike Moriarty, Chair of the Risk Assessment Working Group and Dave DelBiondo, Chair of the Risk Assessment Implementation Subgroup sent a letter to interested parties describing the NAIC's new approach to examinations. In that letter, they explained that:

*"This revised approach differs from the previous examination approach in that the examiner will assess risk throughout the organization on a prospective basis. In accordance with this assessment, not every financial statement account may need to be tested. However, the examiner will be required to provide assurance on the company's financial statements. Overall, the use of the revised risk focused approach will lead examiners to focus on the areas of greatest risk at the insurer and to limit the testing of areas with less risk. In addition, there will be an increased importance in utilizing the work of an insurer's internal and external audit work already performed (emphasis added)."*

Regulatory risks are also receiving greater scrutiny on an international basis. Regulators in the United States have, as members of the International Association of Insurance Supervisors (IAIS), joined their regulatory counterparts from around the world in adopting several supervisory papers at the IAIS Annual General Meeting in late 2008. One of the more important positions as described in the NAIC

release on the meeting focused on how the "standards and accompanying guidance papers address the risk-management practices of insurers, the role of internal models and the necessity of managers and regulators to understand and communicate the results of these tools and practices." (*emphasis added*)

External auditors have been employing a more risk based approach to audits for years to try to reduce the possibility that a material issue would not be addressed in the financial statements. The real issue for insurance executives to focus on now, based on the national and international focus on risks, is how do we leverage the work that our internal and external auditors are performing to satisfy these requirements? The NAIC has made it quite clear that it is critical to have active participation from the insurer in coordinating access to external and internal audit workpapers. Insurers must also be able to assist the examiner in understanding how the workpapers relate to the specific legal entity under examination.

This new approach is more than just a SOX based financial reporting accuracy model; it is a full diagnostic of the inherent risks of the entity. The real issue here is that if management, the Board and the Audit Committee don't specifically set the scope of work to address the requirements of the new risk based examination standards, within the work product required from both internal and external auditors, then examinations can quickly become more expensive. Furthermore, lack of involvement or understanding of these issues could be construed by regulators as an inherent weakness in corporate governance. To address the risks with your internal and external auditors, you must understand what the NAIC defines as key risks. Once you understand these risks, it will enable you to incorporate them into your internal and external auditor's scopes of work. The key risks described by the NAIC's Risk Assessment Working Group are:

### **Credit Risk**

Amounts actually collected or collectible are less than those contractually due.

### **Market Risk**

Movement in market rates or prices, such as interest rates, foreign exchanges rates or equity prices adversely affect the reported and/or market value of investments.



### **Pricing/Underwriting Risk**

Pricing and underwriting practices are inadequate to provide for risks assumed.

### **Reserving Risk**

Actual losses or other contractual payments reflected in reported reserves or other liabilities will be greater than estimated.

### **Liquidity Risk**

Inability to meet contractual obligations as they become due because of an inability to liquidate assets or obtain adequate funding at favorable terms to the company.

### **Operational Risk**

Operational problems such as inadequate information systems, breaches in internal controls, fraud or unforeseen catastrophes will result in unexpected losses.

### **Legal Risk**

Non-conformance with laws, rules, regulations, prescribed practices or ethical standards in any jurisdiction in which the entity operates will result in a disruption in business and financial loss.

### **Strategic Risk**

Inability to implement appropriate business plans, to make decisions, to allocate resources or to adapt to changes in the business environment will adversely affect competitive position and financial condition.

### **Reputational Risk**

Negative publicity, whether true or not, causes a decline in the customer base, costly litigation and/or revenue reductions.

If management and the Board have not discussed these risks yet, we would suggest that you brainstorm and document your responses to the above to use as a focal point for future monitoring activities. We would also suggest that, as an insurance company, you should have an honest discussion with your company designated financial analyst at your domiciled department of insurance to gain an understanding of potential concerns they have related to your company; this discussion may augment or enhance issues already raised during your brainstorming session. Lastly, take a good look at your last two or three examination reports and summary recommendation reports, do they show any positive or negative trends? Are the issues the same or is there improvement? Did the insurance department make a recommendation or require corrective actions that have slipped through the cracks?

Now that you have begun to understand the risks, how do you incorporate them

into the scope of your internal/external auditors work product? To begin with, we would suggest have an honest sit down between the Audit Committee of the Board and both the internal and external auditors to discuss each party's expectations so that duplicative work can be eliminated and complemented by the other party. Define what key policies and procedures are in place to address the aforementioned risks, and then decide who will audit what and how much testing is required to leverage the work of each party. Some suggestions auditing the controls on the aforementioned risks appear below; they are not by any means an exhaustive list, just thought provoking:

### **Credit Risk**

What are our procedures for accepting new insureds and are they being complied with? Are D&B's, credit reports and Lexis Nexus searches performed to ascertain the level of integrity and credit worthiness? Are aged A/R reports run monthly and appropriately followed up on to mitigate credit risks? Are warning letters being generated timely to insured's within regulatory guidelines? Is credit risk reassessed by customer prior to each annual renewal period?

### **Market Risk**

Is the Board reviewing performance of investments with regular frequency? How involved is our designated external investment manager in evaluating and providing feedback to management and the Board on investment quality and volatility; are they investing as the Board has designated? Is our investment manager adequately bonded and/or insured?

### **Pricing/Underwriting Risk**

Do underwriting or the actuaries have all the information/data necessary to price the product? If no competition for a new product exists, has anyone questioned why no other companies are writing the same risk (too risky)? If company market prices and loss ratios are lower than competitive products, has anyone evaluated the reason why? Has data from the claims payment system been reconciled to the actuarial system that is creating the pricing models? Has data for rate filings been compared to past and projected inflationary increases for accuracy? Are initial reserves supported by credible data to assess true projected losses by product or insured; there is nothing worse than finding out two years later that you underpriced risk for that long.

### **Reserving Risk**

Do your reserves have more ups and downs than a roller coaster ride? Have the actuaries reviewed and revised modeling

to reflect known inconsistencies or is it SALY (same as last year)? Have risk models been updated for new products? Are all reserves generated by the company reviewed and signed off by the company's actuary prior to inclusion in financial statements?

### **Liquidity Risk**

Are letters of credit, sources of capital and investments sufficient to meet contractual obligations as they become due? Is there a plan to address both immediate and long term cash shortfalls? Can the company afford to hold an investment until it regains market value in the face of marked declines?

### **Operational Risk**

Have increased pressures related to the economy been accounted for? Increases in property abandonment, inability to make home/car payments and expected increase in workers compensation related fraud should be on everyone's watch list. Lack of funds may have delayed key IT projects that were projected to increase ROI; have these "back burner" projects been reflected in modifications to the strategic plan? Has lack of investment in key IT projects put the company at adverse operational risk when compared to their peers in the market? Have internal controls, both system and soft controls, been updated and tested to determine if they are still performing as designed? Has the company stress tested its assumptions and financials to determine how it would perform in less than optimum market conditions? Have broker and insured portals been secured and encrypted to protect from inadvertent disclosures and/or malicious attacks?

### **Legal Risk**

Has the inside compliance officer and inside/external counsel reviewed the company's compliance with laws, rules, regulations, prescribed practices or ethical standards in every jurisdiction in which the entity operates? Serious fines and the attendant adverse publicity have affected many companies' reputations. Are there any lawsuits that may be pointing to systemic risk that the organization has not bothered to investigate and/or remediate? Does the company have a disclosure notice system and insurance coverage for accidental release or hacking access of sensitive client information?

### **Strategic Risk**

Has the Board been involved in the development of business plans for at least three years out? How active is the Board in reviewing management's decisions to allocate resources, develop



new infrastructure, including IT systems redesign or replacement in order to or to adapt to changes in the business environment? Can the Board and/or management actually articulate to an outsider what the company's strengths weaknesses, opportunities and threats are? For closely held businesses, is there any succession plan? What would happen if the one or two man IT department was involved in an accident tomorrow? Is there a disaster recovery plan and has it been tested?

### Reputational Risk

Couple all of the above with the specter of public disclosure of having all of your company's dirty laundry being aired on the nightly news or in the local news paper. The Board, stockholders, policy holders, regulators and the public will not be amused, the local bar association will be ecstatic (refer to Legal Risk above)!

Once there is a clear understanding of what key risks represent in your organization, we need to determine the amount of documentation that will support controls for each major category. If you have not documented controls thoroughly, now would be a good time to do so. Think of each risk that you have identified then ask how what would be the best control or process to mitigate that risk. For starters, some controls to consider include:

- Active Board and management oversight
- Risk management as a process, not just policy manual on the shelf; it should address monitoring and management of all key information systems
- All service providers are currently covered by recently issued SAS 70s
- Clarity in all policies, procedures and authorization limits
- Documentation of internal controls
- Processes to address all key regulatory and legal requirements required of the company
- Frequent reconciliations of system data to the general ledger and sub-ledgers
- Frequent analysis of any fluctuations in account balances and adequate explanations for the differences
- All employees understand the company's code of conduct and adhere to it

It is paramount that risk management processes are employed to safeguard company assets against unforeseen losses. Many companies think that risk management only applies to the big guys. Under the new risk based audit approach, it applies to all companies; the larger the

company the greater the expectation of adherence but that does not mean a small to medium size company is off the hook. Technically, the smallest companies must also have the same types of controls to manage risk to prevent failure. The very largest companies tend to have well documented controls but that does not assure that they are complied with in all instances; small companies may lack documentation but may be very compliant. Either way, the examiners are coming and their expectations are clearly articulated in the Examiners Handbook. The process of assessing and mitigating risk is not a punitive exercise by regulators; instead it should be viewed as a blueprint for assuring your success.

Internal audit staff, management, board members and the external auditors need to demonstrate to examiners that someone is monitoring existing controls and also evaluating discovered weaknesses and the effectiveness of mitigation efforts. If the company cannot demonstrate these efforts, then examiners will have no choice but to test and evaluate controls on their own which may also increase the amount of substantive testing as well. If the Company does not have the resources to evaluate and monitor controls, it may be much more efficient and cost effective to outsource this activity to a firm that has a strong track record of working with examiners on both IT controls and organizational controls.

An added benefit to assessing and monitoring risk for those that don't believe in the value of the activity was documented by the Marsh/GMI report entitled the "Importance of ERM in an Economic Upheaval." The report cited that well over 80% of large corporations have ERM programs. Their biggest concern and challenge will be how to effectively communicate this data to investors in annual reports and investor meetings. Strong risk management practices assist companies in attracting capital to accomplish their goals. Many venture capitalists, underwriters of public offerings and lending sources that we are acquainted with insist on reviewing the ERM as part of their due diligence. If you have your doubts, in an article entitled "Agencies Jockey Over Evaluation Models" in *Risk & Insurance* ([www.riskandinsurance.com](http://www.riskandinsurance.com)), Patricia Vowinkel discussed how credit rating agencies such as S&P, Moody's and Fitch have adapted their review processes to incorporate evaluation of companies via enhanced analysis of ERM practices.

To paraphrase Tom Cruise in closing, "Every now and then say, "Testing controls." "Testing controls and assessing risks" gives you freedom. Freedom brings opportunity.

*Opportunity makes your future.*