Whitepaper

Enterprise Risk Management & the Compliance Professional

By **Denise Tessier**, Senior Regulatory Specialist, Wolters Kluwer Financial Services

Enterprise risk management (ERM) has become one of the most important and valuable management tools for insurance companies. Increased focus on ERM by regulators, auditing firms, and rating agencies has heightened pressure on carriers to adopt robust ERM programs. Recent developments at both the state and federal, including the NAIC Risk Management and Own Risk Solvency Assessment Model Act, will drive ERM initiatives further. What does this mean for an insurer's compliance function, as a main pillar of the ERM framework?

This Whitepaper will review current regulatory drivers of ERM, the fundamentals of the enterprise risk review process, and the challenges and opportunities companies are facing while trying to integrate traditional compliance activities into a larger ERM program, highlighting the increasingly visible role of the Compliance professional.

Broadening the Compliance Horizon Into an Enterprise Risk View

Enterprise risk management is the process of planning, organizing, leading, and controlling all activities of a company in an integrated fashion, in order to minimize the effects of risk on the company's capital and earnings. While a Compliance team or department typically manages specific kinds of risk to the company, typically risks stemming from specific laws or regulations, an ERM program has a much broader scope. Its view is of the "whole world" of risk throughout a company. Compliance risks are only part of the ERM picture, but they are some of the most significant risks to the company from a financial perspective, ranking high in priority for managerial review and action. The challenge facing many compliance professionals today is how best to integrate compliance risks into a wider world of risk in a formal ERM structure.

Drivers of ERM - Why Should Compliance Care?

For many years, the primary incentives for companies to adopt ERM programs have been mandatory or emerging legal and regulatory obligations – a prime responsibility of the compliance function. These obligations continue to expand rapidly. For example, public companies are subject to Section 404 of the Sarbanes-Oxley Act of 2002, which required U.S. publicly-traded corporations to conduct internal control assessments. In 2007, the Securities and Exchange Commission (SEC), which also governs public companies, increased emphasis on corporate risk assessment, and now specifically requires entities to perform certain risk assessment such as a fraud review, involving estimates of potential (or experienced) related exposure to the organization, and mitigation efforts. The SEC has further issued rules requiring disclosures relating to the extent of the board's role in risk oversight. The New York Stock Exchange corporate governance rules also require that Audit Committees of its listed companies "discuss policies with respect to risk assessment and risk management." Specific requirements vary and should be reviewed for each organization.

Specifically with regards to insurers, nearly all state departments of insurance are now requiring periodic risk-

based exams of insurance carriers of all sizes. While traditional financial examinations focused on historical fiscal information, they provided a picture of a company only as of a point in time. Risk-based exams focus on the risks of the entire company and the entity's solvency in the future, enabling regulators to catch more problems early on. Regulators also now review in more depth overall corporate management strategies, potential future exposures to risk, and loss specific to a company's underwriting plan. They expect companies to have a strong ERM program to identify, mitigate, and manage risk day-to-day, as well as on a strategic basis.

Another major driver of ERM is the recently-adopted National Association of Insurance Commissioner's (NAIC's) Risk Management and Own Risk and Solvency Assessment ("RMORSA") Model Act and its associated reporting. This RMORSA reporting has evolved significantly over the past several years, requiring carriers writing over $500M of direct written premium, or groups writing more than $1B of direct premium, to report to state regulators a detailed review of their solvency position in light of specific risks faced by the company. While the NAIC's recommendations have yet to enacted into law by individual states for an effective date of January 1, 2015, insurers may be expected to have a RMORSA reporting process in place as part of their broader ERM strategy, and establish capital planning in light of their unique risks, by 2014 The NAIC is also coordinating heavily with international regulators to improve consistency with their risk and compliance frameworks, which may impact global carriers.

Further, rating agencies are expecting organizations to adopt robust risk management programs, and will evaluate ERM as part of the agencies' ranking systems. Maintaining strong ratings has been the impetus towards ERM for many carriers who may not otherwise be subject to significant risk self-examination requirements. Standard & Poor's (S&P) has been the most active in promoting the ERM concept. It has developed a detailed eight-part rating framework or matrix, with ERM being a key component. A.M. Best and Moody's have followed with their own analysis tools, and may have differing perspectives that should be uniquely addressed.

Finally, companies are being driven to ERM to further business or financial goals. Leading companies are setting strategic targets for their ERM efforts such as:

- better identification of risks, to minimize "surprises" or shocks to the company;
- beefing up controls and risk mitigation techniques;
- achieving cost savings and efficiencies, by better ranking competing risk and control priorities, and allocating resources to higher priority items more effectively;
- improving the capital planning process;
- securing a reputational or competitive advantage, by leading the adoption of industry ERM best practices.

An effective ERM program can also help steer the direction of the organization, helping to identify what business, products or services to grow. Risk management not only protects revenue, but ultimately provides the company with new ways of seeing opportunities.

Moving Compliance into a Wider World of Risk - The ERM Framework

Adopting an ERM program, and looking at risks through multiple perspectives across the organization, is often a major cultural change for many companies. For the Compliance team, an ERM initiative can lead to new ways of looking at compliance risk, as more attention is paid to a thorough quantification of risk, as well as the ripple effects a compliance breach may have in other departments or functional areas such as claims, underwriting and finance. There are many benefits to Compliance from the establishment of an ERM framework, as noted below. But first, an introductory description of an ERM program may be helpful.

The first step in the ERM process is generally a "risk assessment" phase, identifying current and emerging risks by business unit or department. A "risk library" or "risk register" listing all risks of the company is the ultimate product of the assessment phase. This can be accomplished via face-to-face interviews or group meetings, surveys or questionnaires, researching industry press, and by using experts and consultants. In the risk assessment process, even the smallest tidbits of information about potential sources of loss are important to help identify patterns and trends.

Risks are also reviewed with respect to their impact on other company operations or departments. For example, the risk of a compliance breach, such as failure of an appointed broker to adhere to producer licensing laws, may result in a direct statutory financial penalty or fine charged to the company as a result of a market conduct exam, but may also have a knock-on impact to:

- affected underwriters, in the form of a lost business partner relationship, and future revenue stream;
- the Legal department, if litigation ensues relating to the broker violation;
- Marketing or and Public relations staff who may need to manage press and public relations communications regarding the issue;

- Accounting, to the extent that reconciliations or other financial transactions need to be carried out to verify producer cash flows or terminate banking relationships.

Once risks are identified, they can be scored or rated, and prioritized by their significance. Resources and activities can then be focused around the most dangerous risks, and the most beneficial controls. To this end, companies establish standard scales and metrics for evaluation of different risks for like-to-like comparisons. Metrics complimenting or completing risk analysis commonly include:

- Frequency: This is the likelihood of a risk occurring, usually classified on some scale from "very unlikely" to "very probable;"
- Severity, or Magnitude: This measures of the impact of the risk should it occur, or a consequence. Severity is also measured on a continuum of potential loss, from insignificant or immaterial, to extreme.
- Velocity & Duration: How fast might a loss happen? How long will it last? A natural disaster will likely have an extreme, sudden impact, whereas poor business conditions or increased competition may be just as damaging, but may build up, peak and run down over much longer period of time, potentially offering more time to implement loss mitigation techniques or make strategic management changes.
- Degree of Causation or Connectivity: Is the risk one which may have waves of impact in multiple areas of the company? For example, an internal bookkeeping error may only affect the finance department, whereas a failure to follow underwriting guidelines or protocols could have an impact not only on the underwriting department, but could lead to an increase in claims, fines, fees or penalties, and could lead to legal or regulatory issues. Controls should exist to prevent both types of losses, but with a limited amount of time and money, the company may choose to address the latter situation first.

Once risks are assessed and prioritized, the next step is to catalog the company's controls, the specific techniques, policies, and procedures which are used to reduce or mitigate identified risks. Even the most effective controls won't necessarily eliminate 100% of all risk, but well-developed, sustainable controls will have a direct financial impact on a company, helping to prevent large losses, or regulatory fines, fees or penalties.

From the implementation stage, and continuing as long as the program is running, an ERM program should have planned milestone for participants to evaluate prior work - successes and failures - and make adjustments. Risk monitoring protocols should be scheduled on a regular basis, so that risks can be reviewed, re-ranked, and controls can be tested and tweaked. Monitoring regulatory change is also important, to consider how new laws and proposals might impact risks and controls within the ERM program.

Most ERM programs also have a robust reporting component. Reporting of risks, controls, and prioritization results is typically made to multiple levels of management, with information about risks and controlled tailored to each group. Some reports will be very high level, summarizing the very top risks and controls for the company. Other detailed reports might be run for specific risks sorted by department, line of business, or by legal entity.

Finally, with all of the above information at hand, knowing the full range of risks it faces, and controls at its disposal, the company can tackle some practical business decisions. In the final strategic analysis phase, managers may discuss the allocation of company resources, and evaluate whether potential gains will outbalance losses in a proposed course of corporate action. ERM strategic analysis can be used to help answer questions such as:

- Should we enter into a new line of business or develop a new product?
- Should we expand and open a branch office in X location?
- How much capital should the company hold in reserves?

Having strong controls which mitigate the "downside" of risk, a company can then focus on the "upside" of risk — potential opportunities.

The ERM Process – Benefits for Compliance

Prior to the implementation of an ERM program, companies often approach risk control and compliance activities with a "siloed approach;" that is, there is little or no collaboration or standardization of mitigation techniques or controls between business units. Risk assessments are typically done – if at all - informally, with rough qualitative measures, rather than with consistent quantitative guidelines. Risk management efforts often focus disproportionately on risk avoidance techniques and reactive risk controls, rather than proactive, preventative measures. Frequently, risks are identified but are not assigned specific owners who are responsible for mitigating or improving the risk situation. And too often, risks are only ultimately perceived as threats, when they also could present significant opportunities for the company.

Bringing risk management in multiple departments into one ERM program or function significantly improves the company's chances of managing risks well, and can particularly help the compliance function do its job better. Insurers need to have a consistent and standard approach to risk throughout their organization. When they achieve this, particularly when facilitated by procedures and technology that help them centralize the process, companies benefit from having a more transparent view of risk within their organization.

Foremost, having an ERM program broadens the relationship between Compliance and other business units in the organization. Discussions of potential loss faced across the enterprise by an action, event or activity can deepen all participants' understanding of inter-dependencies between departments. Legal, regulatory, and compliance staff or functions, where previously segregated or siloed, become more aligned, facilitating the sharing of information on issues of common interest. Communications and overall relationships may also improve between Compliance and other operational areas like Underwriting, Claims, and Finance, as all areas come to better understand each others' concerns and priorities.

As a result, implementation of a formal ERM risk assessment process often provides new perspectives on how information about the company's risks should be organized and managed, particularly compliance risks. This new perspective often leads to re-assignments of resources and staff responsibilities, warranting new or revised workflows, managerial approval procedures, or attestation processes.

Further, when the calculation of risks and the costs of controls can be measured in dollars, priorities can more easily be set. ERM highlights areas where additional staff/time/money is needed. It also encourages the strengthening of controls, particularly compliance-related measures, and offers an opportunity for the company to implement "best practices" with respect to its day-to-day policies and procedures. In many cases, adopting a strong ERM program can increase the profile and value of the Compliance function itself, as the Compliance department often leads significant operational improvement projects identified by an ERM team.

Challenges for Compliance when Adopting ERM

Although there are many advantages of adopting ERM, the process is not always easy or smooth. There are several challenges in designing an ERM program which may particularly impact or affect the Compliance team.

Challenge #1: Defining the Compliance Function Itself

An initial problem is how to define the "Compliance" function itself. One of the first tasks in setting up an ERM program is to identify and segregate the major operational areas or functions in the organization which share the same type of risk, into discrete "Business Units" or organizational units. The hierarchy of responsibility for risk in an ERM program may or may not match named Departments in the company, or what human resources would put into an organizational chart for other business purposes, but is an allocation solely for the identification, management and control of common risks.

There are a number of ways to define how "compliance risks" will be managed within an entity, and each company is different. The process of determining who should be responsible can be difficult, requiring significant discussion and thought. The architect(s) of the ERM program must fully explore the question of who is already responsible for what risks, and what controls, and who SHOULD be responsible for them in the future? The range of risks that could be considered "compliance risk" is very broad, and may include, for some companies:

- Violation of the company's Code of Conduct and Ethics;
- Failure to adhere to state laws regarding advertising to and communications with policyholders;
- Non-compliance specifically with policy rate and form filing procedures;
- Violation of "good-faith" claim handling laws and regulations; or
- Breach of internal underwriting guidelines and authorities.

In this process, there is often a lot of overlap and duplication of duties and roles, particularly between the Compliance, Legal, Operations, and Human Resource Departments.

For example, some companies may make a distinction between management of "internal controls" created from company-specific policy preferences, and "external controls" that are created as a result of specific legal or regulatory requirements, so that the Compliance team is assigned to managing internal policies and procedures, while the Legal team manages new laws and regulations. In other companies, a Compliance team may be tracking new laws and regulations, but the Law Department is responsible for other functions such as corporate contracts or licensing, or may be charged with developing day-to-day policies and procedures once Compliance passes on news of legislative changes. As another example, the company's Code of Ethics and Conduct may be drafted, monitored and enforced by the Law Department, a Compliance Department, Human Resources – or all three.

Drawing out the various possible combinations of risks, controls, and associated responsibilities can be one of the most confusing and time consuming phases of developing an ERM program, and the Compliance function is usually the most difficult to color in effectively – often remaining a "grey area."

Challenge #2: Keeping Risks and Controls Updated to Reflect Regulatory Change

A second major challenge to Compliance is keeping abreast of changes in compliance and regulatory risk, once they are identified or defined, and carrying that through to the ERM program. When new products and services are being offered, or as laws and regulations change, the company must re-define what "risks" are being tracked in the ERM program, re-score or re-prioritize the risks in terms of their significance to the company, and revise any controls used to mitigate them. The Compliance team is often responsible for this ongoing risk/control review in the ERM process.

Insurers are constantly bombarded with changes to compliance and regulatory risk from multiple sources – the laws and regulations of 50+ states, the U.S. federal government, and international authorities - as well as facing related risks such as consumer complaints, and market conduct fines, fees and penalties. Over 11,000 new laws and regulations specifically relating to insurance are proposed in the U.S. each year, with over 3,000 laws finally enacted or adopted. From an ERM perspective, the pure number of laws and regulations can make it difficult to enunciate concise standard risk definitions or categories.

Likewise, it may be difficult to craft ERM controls that are broad and flexible enough to adjust to frequent changes in legal requirements. Regulators also may change their degree of scrutiny of certain kinds of activities or practices, so that a relatively low risk to the company one year might be a high risk to the company in another year. As an example, the risk of data breaches has become an increasing concern to insurers over the past 5 years. It is predicted that IT security-related risks and control costs will raise even further, as regulators and legislators focus their radar more on consumer privacy protection issues, drafting more stringent cyber security laws.

The Compliance professional can play a key role identifying current compliance regulatory risks - not just for the Compliance department, but for other affected areas, such as Claims or Underwriting. Having a solid process, reliable internal procedures and workflows for tracking regulatory change by the Compliance team can help streamline the ERM process as well, and ensure that it is as complete and up-to-date as possible.

Challenge #3: Assessing Risk Frequency & Severity for Compliance Functions

Quantifying risk may be another special challenge for Compliance in the ERM process. Compliance professionals may be well used to identifying and documenting compliance or legal risks, but may or may not be used to evaluating risk frequency or severity, or prioritizing the many and varied compliance issues need to be addressed, particularly as respects departments outside of Compliance which may be impacted by a compliance breach. This depends on the company. Some companies have a "zero tolerance" rule to compliance or regulatory violations, and try to be 100% compliant with every law, to the letter, despite the potential likelihood of a fine or loss related to any violation. Other companies may do some cost-benefit analysis of implementing controls, but have difficultly allocating money or time to control functions when faced with several risks perceived as equally dangerous or significant.

The Compliance department may be somewhat at a natural disadvantage when in assessing individual risk. For Underwriting risks, risk magnitude might be a factor of policy limits, or aggregation of limits for a line of business, and there is usually system data which can support a rough estimate of severity as well as frequency of loss. Similarly, Claim staff usually have a wealth of historical claim file records, internal system data about loss history, and external industry statistics which can serve as a basis for a financial estimate of particular risks. It is also extremely difficult to quantify how compliance, legal or regulatory risks might be aggregated if they affect a number of departments across the company.

There are, however, a few resources which may assist Compliance in this assessment process. Laws and regulations may, in some cases, specify any fines, fees or penalties for a breach. State Department of Insurance websites and third party databases are available which disclose the results of past market conduct exams. This information often includes the financial penalties or license actions taken for violations. And finally – although this is, of course, the least preferred data source – the company may have tracked its own history of compliance breaches, either breach which lead to actual financial losses of some sort, or "near misses" which could have spawned claim, regulatory or legal action. With the implementation of ERM, the Compliance team may need to be more alert to such resources to assist with ERM risk reviews.

Challenge #4 – Identifying and Implementing Best Practice Controls

"Policies and procedures" are one of the most important kinds of ERM "controls," yet many companies seeking to implement ERM programs act as if the two concepts are separate and unrelated. In some companies, the Compliance department, responsible for daily policies and procedures, and risk management staff documenting company-wide ERM controls, are in two different departments, engaged in a tug-of-war, competing for attention and resources.

As noted above, as part of their ERM efforts, companies typically create a list or library of internal controls, all the measures taken by a company to manage risk. They can include such things as management approval hierarchies, IT security efforts, business continuity or backup plans, and outsourcing strategies. Ideally, companies should identify one risk register and one set of controls for the enterprise as a whole, making them easier to manage and measure over time, providing significant operational efficiency and save time/money in the long run.

"Policies and procedures" are a key subset of controls. They help manage potential losses from financial, underwriting, regulatory, or claims activities. Historically, companies have catalogued compliance standards and behavioral guidelines into policy manuals or handbooks. For each policy setting forth general and goals guidelines for behavior, there is usually a corresponding written procedure which documents the actual day-to-day, nitty-gritty steps of how to comply with such policies. Frequently, this is the responsibility of the Compliance team to manage.

In theory, policies and procedures should be an integral part of a company's ERM efforts. In practice, however, the some insurers have lists or libraries of policies and procedures, and a separate database of ERM risks and controls, with no integration or cross-checking of the two. On one side, there is day-to-day departmental compliance. On the other side, there is the ERM program. This dichotomy can arise for several reasons:

- The ERM program may have been started up as a side-project of another department such as Finance or Internal Audit, not fully attuned to the integration of policies and procedures from a Compliance perspective;
- Companies getting up to speed on ERM may quickly develop a library of generic industry-standard risks and controls, just to get their framework started, without first thoroughly reviewing all of their own historical policies and procedures.
- Certain historical policies and procedures themselves may be outdated, without ownership or roles assigned, may be housed in multiple places, and may no longer serve as effective or appropriate risk mitigators - never making it into the ERM control library.

As a result, separate compliance and ERM workflows may be established to address the same or similar risks. Two completely different sets of attestation and sign-off protocols may exist for routine compliance versus ERM control purposes. Managers and staff responsible for complying with and/or attesting to the operation of controls and success of procedures may be confused as to what to follow, how to attest to each, and may be frustrated by duplication of review efforts. Costs may double. Audit efforts may multiply. Compliance procedures may not clearly map to loss events, issues or incidents tracked in the ERM process, and specific policy or workflow failures can be hard to identify. Laws, rules and regulations may not be adequately or consistently followed, and changes in laws may not be properly assessed or implemented.

All of the above can affect the Compliance team, who may get complaints from staff first, being "on the front line." On the ERM side of the equation, risk may not be sufficiently evaluated and overall risk mitigation efforts can collapse.

Ideally, the goal should be to create one integrated, cohesive set of risks, controls, policies and procedures. ERM controls, and day-to-day policies and procedures, should be synergetic. The Compliance function should, instead, be a main pillar of an ERM program, and solid compliance risk management should be a starting point, and lead the way to, broader enterprise-wide risk management. There are software tools being developed today that can help structure and streamline this process, designed to easily map or cross-reference ERM-library risks and controls with other compliance "policies and procedures." But even a manual process for cross-checking both is helpful. The expense and effort to complete a matching process early in the development of an ERM program will be well repaid over time, making the Compliance job easier as well

Integrating Compliance into ERM Efforts – Recommendations

To meet these challenges, everyone involved in ERM and Compliance efforts should work together, aligning themselves in a common framework, with common goals, and a coordinated approach. To this end, recommendations for increased coordination include:

- The Compliance team should be given more advance notice of, and more information about, new product lines, business partners, vendors, and other strategic issues faced by other departments. The more information Compliance has, and the earlier they have it, the better Compliance staff can assess related compliance or regulatory risks and controls, to offer meaningful input into any decision-making process. Managing the compliance risk of any new business initiative is usually a key first step on the road to success.
- All departments should coordinate efforts on identifying and sharing "emerging risks" and trends in their area of responsibility, and create a communication loop to understand risks seen by other areas (legal, finance, etc.)
- Use Compliance team members, as leaders or participants, in ERM projects such as reviewing or auditing certain cross-departmental controls, developing key performance indicators, or improving management ERM reports.
- Better integrate ERM and compliance "policies and procedures," making sure where there is an ERM "risk" there is a matching "control," that such control is documented in more detail in a policy and day-to-day procedure (typically owned by the Compliance team). If there is a daily policy or procedure, what "risk" is it trying to control? See if there are any gaps or areas of duplication.
- Widen the audience who receives news of compliance breaches, and increase focus on the "group-wide" impact of compliance violations. This will help the ERM team and management see compliance problems from multiple angles, in terms of the potential harm to the company's reputation, loss of business, and strained agent, broker or reinsurance relationships. Communication of how compliance risks actually develop, and how they are managed or dealt with in practice, helps educate other departments about losses inherent in the business, and potential solutions for mitigating future losses.

Despite the challenges that the Compliance department may face while implementing an ERM program, they can also provide crucial skills, wide perspective and valuable insight to help a company assess legal and regulatory risk. Solid compliance risk management is crucial to enterprise risk management, and can provide a strong foundation for broader evaluation of risks and controls across the company. Compliance professionals should be star performers on every ERM team.

Wolters Kluwer Financial Services is a comprehensive regulatory compliance and risk management business that helps financial organizations manage operational, compliance and financial risk and reporting, and improve efficiency and effectiveness across their enterprise. The organization's prominent brands include: FRSGlobal, *ARC* Logics® for Financial Services, PCi, Compliance Resource Network, Bankers Systems, VMP® Mortgage Solutions, AppOne®, GainsKeeper®, Capital Changes, NILS, AuthenticWeb™ and Uniform Forms™. Wolters Kluwer Financial Services supports its global customers with more than 30 offices in 20 countries and is a leading worldwide provider of compliance and risk management solutions for the financial services industry, serving more than 15,000 banking, insurance and securities customers across the globe. Wolters Kluwer Financial Services is part of Wolters Kluwer, a leading global information services and publishing company with annual revenues of (2011) €3.6 billion ($4.7 billion) and approximately 19,000 employees worldwide. Please visit our website for more information.

Wolters Kluwer Financial Services
130 Turner Street, Building 3, 4th Floor
Waltham, MA 02453
Phone: 866.221.0404

Wolters Kluwer
Financial Services

To learn more visit
WoltersKluwerFS.com/*ARC*Logics