

**About the Author**

**Kevin M. Madigan**  
PhD, ACAS, MAAA

Mr. Madigan is a Consultant with Pinnacle Actuarial Resources, Inc., in its Saratoga Springs, NY office. He is an Associate of the Casualty Actuarial Society (CAS), a Member of the American Academy of Actuaries (AAA), and an ARIAS-US Certified Arbitrator. He is currently chair of the Joint CAS/SOA Committee on the Enterprise Risk Management Symposium, is a member of the ERM Task Force of the ASB, and a member of the CAS Economic Capital Model Working Party. He holds both a Ph.D. and an M.A. in Mathematics from the State University of New York at Albany, and a B.S. in Mathematics from Auburn University.

Mr. Madigan is a frequent industry speaker on a variety of topics, including ERM, and he co-authored the paper "Reserving for Asbestos Liabilities", which appeared in the Fall 2003 CAS Forum. Mr. Madigan's ERM consulting practice has thus far included DFA modeling, capital adequacy analyses, issues regarding property catastrophe exposures, economic capital modeling, and the education of client's management and personnel regarding the fundamental principles of ERM.

Mr. Madigan may be contacted at  
518 · 288 · 0139  
kmadigan@pinnacleactuarials.com

**An Enterprise Risk Management Primer**

By Kevin M. Madigan, PhD, ACAS, MAAA

Enterprise Risk Management (ERM) continues to be a very popular and important topic. Senior managements, boards of directors, rating agencies, regulatory bodies, professional and trade associations all seem to have an insatiable appetite for discussions and debates about ERM. Typing "enterprise risk management" into one's favorite search engine returns hundreds of millions of web pages. Many firms have already successfully implemented ERM programs while those that have not are feeling pressure from their boards and other stakeholders to do so immediately – or at least as soon as possible. ERM is not a passing fad; it has become an essential element of good management practice.

ERM is simple to say and fairly easy to explain and understand, but the three letter acronym does not mean the same thing to everyone. There are significant disagreements among "ERM experts" as to the proper focus of a successful ERM program. Some claim – incorrectly – that ERM is part of the Governance, Risk and Compliance (GRC) framework. Others point out that for many organizations and many of the risks they face, governance and compliance are small parts of ERM, while in other settings a GRC approach may be sufficient for managing the largest risks facing the organization. It is easy to become overwhelmed by the details.

There is something unique about every organization; many of those

unique aspects are fundamental and must be considered when developing an appropriate ERM program. There is no "one size fits all" approach and no such thing as "the one, true path". In particular, an ERM program must be appropriate to the **size, scale** and **complexity** of the risks faced by the organization for which it has been developed.

“ERM is not a passing fad; it has become an essential element of good management practice.”

The inappropriateness of a manufacturing firm blindly mimicking the successful ERM framework of a bank, or of a publicly traded insurance company merely grafting the ERM framework of a non-profit trade association onto their organization should be obvious. It would be equally inappropriate for an Excess and Surplus Lines writer to mimic the ERM program of a highly regulated multi-line global insurer or for a workers' compensation captive insurer to model their ERM program after one successfully implemented by a property catastrophe reinsurer. Even organizations that view themselves as operating "in the same space" have differing attitudes towards and tolerances for risk – mutual insurers compared to stock insurers being an obvious example – and their ERM programs must reflect these differences.

Furthermore, it is important to remember that some risks bring opportunity, but not all do so. Some risks do not and never will bring upside opportunities commensurate with the downside possibilities.

As organizations begin to apply the details discussed below it is helpful to remember a few basic ideas:

- The chances for a successful implementation of ERM will be higher if one starts with what is known and is already being done well and uses this as a foundation upon which to build.
- One can begin to close the gaps by applying what has been learned from prior success coupled with new knowledge and data.
- Successful ERM approaches tend to be iterative, continuous processes with feedback loops that incorporate what is learned along the way.
- One should never lose sight of the 5 keys of traditional risk management: identify, assess, evaluate, mitigate and monitor.

## Culture

Despite the necessary differences between specific ERM programs employed by particular organizations, the challenges, and the seemingly overwhelming complexities involved, there are several bedrock commonalities that can be relied upon to make implementation tractable and practical.

Let's start with a bit of very encouraging – but not fully appreciated – information: most organizations are already “doing ERM” to some extent. Furthermore, it need not be any more difficult than the challenges that successful organizations have already learned to confront.

It is important to recognize – and internalize – the fact that the ‘M’ in ERM stands for Management, not compliance and not risk modeling. Just as organizations were managed before Management became a subject of study in the late 19th and early 20th centuries, the ERM label does not create something that didn't exist before. It brings focus, richness, and depth to something that was already there, brings it into the light and promises to help us develop better ways to manage our organizations. And just as the theories underlying the management of organizations are still evolving after more than 100 years of intense study, ERM will continue to evolve during the next several decades. Boards of directors and C-suite professionals understand that one is never “done” managing an organization; there are always improvements that can be made, issues to be dealt with, challenges to be met, and opportunities to exploit. The same is true of ERM – it is never “finished”.

Thus it is critical for organizations to recognize that ERM is not a one-off task or a “flavor of the day” that will fade from memory with the passage of time. Appropriate resources and

focus must be brought to bear. This includes commitment from all members of the senior management and the existence of an identified individual at the appropriate level in the organization who is accountable for implementing and overseeing the ERM program. This person's title (Chief Risk Officer?), other responsibilities, place within the organization and the need for a dedicated ERM staff all depend upon the specific risks faced by the organization. No matter how it is done, the existence of an “ERM champion” within the organization, someone who is held accountable for successfully implementing ERM, is crucial.

Successful ERM implementation requires an appropriate environment in which ERM can flourish. Risk language and an open minded attitude towards learning, making use of new information and hard earned lessons can greatly enhance the success of an ERM program. Organizations should explicitly strive for clarity in all risk related vocabulary. Management should avoid the use of different words for the same ideas or the same words for different ideas, even in

seemingly inconsequential matters. For example, many people consider “risk” to have no positive attributes; such people use the word only when discussing strictly negative outcomes. Others use the term “risk” to represent uncertainty in outcomes, encompassing both negative and positive outcomes. There are similar issues with the words “loss” and “losses”. Outside of the P&C insurance industry these words represent

bad outcomes, whereas within the (US based, at least) P&C insurance industry these words do not have such negative connotations – unless the losses are higher than expected. Some people prefer to use the words “claim” and “claims” to represent loss payments while others use those words to represent notices of claims. These may seem like trivial matters, but if the people within an organization do not use language consistently then the organization faces a larger than necessary risk of miscommunication.

Efficient and effective communication is an essential component of ERM, and so care should be taken in the words that are used to convey ideas, directives, policies, procedures, goals and strategies, etc. At the same time, the focus on semantics should not be so overpowering that it stifles the creativity and innovation necessary for the organization's success. This can be a tricky balancing act but is well worth pursuing as clarity in language is itself a good risk management practice, helping to mitigate the dangers of miscommunication and misunderstanding.

### ERM Cultural Issues

- Accountability
- Authority
- Communication
- Long Term Commitment
- Language
- Learning Environment

The organization's culture must allow for learning and improvement at all levels. Again, this environment needs to be tailored to the size, scale and complexity of the risks faced by the organization. Rigid compartmentalization and silo approaches should be avoided (as appropriate), with "big picture" approaches and knowledge sharing being encouraged. Integration of people and ideas within and across the enterprise is good management practice in general, and helps to create an environment where ERM can grow and be successful.

A last note on culture: studies regarding risk perception amongst individuals and groups have shown that attitudes towards risk fall into four broad categories:

1. Those willing to take large amounts of risk in pursuit of high returns (with a focus on properly pricing risk and an attitude that there are no bad risks, only underpriced ones – a good approach during economic booms);
2. Those who fear risk and uncertainty (with a heavy focus on avoidance and mitigation – an approach suitable for economic downturns);
3. Those who are convinced that the future is unpredictable (leading to a desire for maximum flexibility and diversification – an approach well suited to times of high economic uncertainty); and
4. Those that seek to optimize the balance between upside and downside risk (a good approach during periods of economic stability).

Only the fourth risk perspective is compatible with the "risk management" approach propounded by many ERM practitioners.

All of these risk attitudes exist inside most organizations, and they are all appropriate for certain risks or certain economic situations. It would be prudent for any ERM program to allow all four of these risk attitudes a place at the decision making table and ensure that they have voices that will be heard. It is much more important for all of these perspectives to be heard and valued than it is for all stakeholders to agree with all of the decisions made by the ultimate decision maker (usually the CEO or Chairman).



## Risk Appetite, Targets and Tolerances

The starting points in the development and implementation of any ERM program are the identification and quantification of the risks faced by the organization. We discuss this in the next section. Once risks have been identified and measured, then the real ERM work can begin: the enunciation and documentation of the organization's risk appetite, the development and enunciation of risk tolerances and risk limits, and the management of risk within these constraints.

The organization's goals and plans should be very closely aligned with its risk appetite. Risk appetite is simply how much risk an organization is willing – and able – to assume. It exists with or without the existence of a formal ERM program. Clearly enunciating it allows an organization to begin managing risk at the enterprise level.

Limits should be clearly defined barriers that the organization does not wish to cross, and tolerances define the area within which the organization is comfortable. Tolerance is akin to a guard rail along a steep and windy road whereas limits are akin to the lane markers. One will normally be safe in their travels if they stay within the lane markers, but breaching the guard rails can be very dangerous – sometimes with catastrophic results.

### Primary Stakeholder Focus

For an ERM program to be most effective, it is imperative that the focus be on the risks that are important to the primary stakeholders. In the for-profit sector, both publicly and privately held firms, that translates to a focus on managing risk to maximize shareholder value. For mutual insurers and reciprocal exchanges the focus would be on maximizing the value as perceived by their policyholders. For other non-profit entities, things can be a little less obvious. For example, management and employees of a risk retention group (RRG) may feel that a priority risk to the organization is competition from private insurers, enticing members to leave the RRG and buy insurance in the private market. Many members of the RRG may not view this as a significant risk, as they may have always wanted to buy private insurance. Those members who prefer the alternative insurance market to the private insurance market, on the other hand, may very well feel that this is a material risk, as the departure of a significant number of members could drastically alter its capital position and risk profile. Another example is charitable organizations that serve more than one distinct group of beneficiaries. An ERM program for such organizations should focus on managing risks so as to maximize the value of the organization to each of these groups of stakeholders.

All aspects of an ERM program, and particularly the risk metrics chosen to measure and identify the priority risks, should be focused on the organization's value to its primary stakeholders.

The following are examples of the kinds of questions that could be asked in this process:

- With which kinds of risk are management and other stakeholders comfortable?
- Which risks keep management up at night, but are nevertheless manageable?
- Which risks should be avoided? Regulatory, pricing, underwriting, reserving, counterparty, catastrophic, investments, marketing, operational and strategic are examples of the risks to consider in this exercise – there are others.
- Is there a target annual return distribution? If so, what kinds of probabilities make management and other stakeholders uncomfortable (e.g. an x% chance of losing y% of capital, an x% chance of missing plan by y%, etc.). Are the stakeholders willing to accept volatility in pursuit of large gains? Are survival and stability more important than growth?
- How much exposure to catastrophic loss (wind, water, fire, earthquake, etc.) is acceptable and how comfortable are management and other stakeholders in relying on exposure models to measure this risk? Should hard maximum limits per zip code, county, state, or region be established to manage this risk?
- How reliant upon reinsurance does an insurer wish to be? All reinsurance contracts carry counterparty risk, and some lines of reinsurance have very pronounced pricing cycles.
- Should some risks only appear on one side of the balance sheet?
- Are there key individuals within the organization whose departure would cause significant disruption? Are there such key clients, competitors or strategic business partners? If so, is this risk fully understood and properly managed?
- In broad terms, what do stakeholders want the organization to be over the short to medium term? What motivates them? For insurance companies, one could rank order things like surplus growth, premium growth, policy count, preservation or enhancement of reputation. In other words, “who are you” and how does that measure up to what the stakeholders want the organization to be?

The above list is illustrative; it is neither proscriptive nor exhaustive.

Risk appetite, limits and tolerances cannot be notional constructs that are only discussed by those at the top of the organization. They need to be communicated widely and care should be taken to ensure that they mesh well with the organization’s culture and stated goals. If the organization’s goals are in conflict with the documented

## Operational and Strategic Risk

Strategic risk (risk surrounding the formulation or implementation of strategy) and operational risk (risk related to the organization’s operations, such as human resources, disasters, fraudulent employees/management, IT, etc.) are of paramount importance in any ERM program. Numerous studies of publicly traded companies experiencing significant declines in shareholder value have shown that in the overwhelming majority of cases these declines were driven by strategic and/or operational risks. Surveys of managements and boards show that these risks are their biggest concerns. Although quantification of these risks can sometimes be difficult, ERM programs must not ignore them.

risk appetite, limits and tolerances, then a few outcomes are highly probable. The most obvious one is that the goals will take precedence, making the ERM program very ineffective (consider the activities within the banking industry in the years leading up to the most recent global recession). Another possibility is that there will be some teeth to the ERM program and the goals will not (more precisely, cannot) be met. The optimal outcome cannot and will not be achieved if the organization’s objectives are in conflict with the documented risk appetite, limits and tolerances. After all, employees’ performance appraisals, career opportunities and near term compensation are all tied closely to those goals.

Employees generally do what they are paid to do, not necessarily what they are told to do. This fact leads to two important, but often overlooked, questions:

- Does the organization’s compensation plan support its goals, and risk appetite, limits, and tolerances, or does it undermine them?
- Are the goals, risk appetite, limits and tolerances compatible with the organization’s culture?

Compensation and organizational goals must be aligned, and the goals must be aligned with the risk appetite, limits and tolerances. For example, underwriters and producers whose compensation is driven by revenue are less likely to alert management to softening market conditions (and recommend appropriate action) than those who are rewarded for bottom line results and are empowered to shrink books of business without negative personal consequences.

## Risk Identification and Measurement

Of course, it is not possible to do any of the above until the risks facing the organization are identified. Limits and tolerances won’t really make any sense in the absence of well defined measurement procedures, or risk metrics. Organizations with successful ERM programs have developed robust risk identification protocols and employ

measurement methodologies that are understood by the appropriate decision makers. All ERM programs require the systematic identification, classification and evaluation of the key risks facing the organization. There are many approaches that can be employed, but as with all things ERM it is imperative that the approaches selected are appropriate to the organization's risk profile, and that risk is measured and evaluated in a consistent way across the organization.

It is important to focus only on the key risks facing the organization. An ERM program that attempts to identify and measure all risks is destined for failure, as it will surely devolve into a burdensome, time consuming compliance exercise. The raison d'être of ERM is to manage risk - not merely to identify and measure it. A successful ERM program provides actionable intelligence to decision makers in their pursuit of the organization's goals. Therefore, one must avoid the temptation to catalog all risks and must instead focus only on those key risks that threaten to impair the attainment of the organization's goals (downside risks) OR that provide opportunities to achieve or exceed those goals (upside risks).

In the arena of risk measurement there are other temptations to avoid. "Delusional exactitude" - convincing oneself of the precision of risk calculations - is an occupational hazard for those that model and measure risk. One must not lose sight of the very basic significant digits rule, and one must never treat a "black box" model as an oracle with answers to all of the important questions. Models are idealized representations of reality, and they all have their weaknesses. The famous aphorism that "all models are wrong, some models are useful" is as true today as it has ever been. In addition, over-reliance on a single method of risk measurement, with no appreciation for the results produced by other methods, can easily lead to sub-optimal risk management - sometimes catastrophically so. Prospects for successful ERM are greatly enhanced with the utilization of more than one risk measurement approach, in models that are no more complex than is required by the risks being measured, coupled with a recognition

that the models provide information and not answers. One must never forget that the whole point of ERM is to provide information to decision makers in pursuit of the organization's goals.

Is an economic capital model necessary for ERM? Again, this depends on the risk profile of the organization. For many insurers the answer is a resounding "yes", while for others it is not so clear. One of the most useful outcomes of implementing an economic capital model is the impact that the process has on all of the cultural issues discussed above. The process of constructing a best practices economic capital model requires communication across the enterprise, development of risk measures, enunciation of risk appetite documentation, and really brings ERM to the forefront for all of the key decision makers and many other stakeholders. This is a powerful argument in favor of going down the economic capital modeling road, but one must also consider the total expense of building and maintaining an economic capital model in relation to the promised benefits.

The introduction of another model into the management process presents new risks, as many organizations discover when they find themselves relying too much on a model. It is probably true that a multi-line insurer cannot realize the full potential of ERM in the absence of an economic capital model; it is also true that a small regional writer of a small number of similar products should focus on other low hanging ERM fruit before embarking on an economic capital modeling project. The owners of a single parent captive insurer could, in all likelihood, benefit considerably from the construction and maintenance of an economic capital model. It truly is a function of the organization's risk profile.

### Controls and Governance

None of ERM practices discussed above will be of any use without appropriate controls and governance procedures. Authorities must be clearly delineated and communicated, and procedures to resolve breaches of limits must be in place. Well understood methods for controlling and governing the risks of the organization are key elements of all ERM programs.

ERM

#### A successful ERM framework is one in which:

- The risks facing the organization are identified and understood, with agreed upon and well understood metrics for measuring those risks
- Management understands and enunciates the organization's risk appetite
- This well understood risk appetite allows for the enunciation of risk targets and risk tolerances
- Limits, controls and governance have been implemented so that the organization's risks stay within the tolerances - or can be managed when they fall outside - with the goal of meeting the risk targets
- Common language and measurement are used to monitor and govern identified risks and to build a culture of risk management and learning that helps the organization achieve its objectives



PRESORTED  
FIRST-CLASS MAIL  
U.S. POSTAGE PAID  
BLOOMINGTON, IL  
PERMIT NO. 111



Scan for Pinnacle's ERM expertise

## PINNACLE Monograph

[pinnacleactuararies.com](http://pinnacleactuararies.com)

### Conclusion

Enterprise Risk Management is not a fad, and for insurance companies it is quickly becoming a requirement. Regulatory and supervisory regimes across the globe are focusing on ERM and soon insurers will be required to demonstrate to their regulators that their ERM programs are sufficient for the risks they face. Many firms are already well down the ERM path, several are quickly catching up, while others are only just beginning the ERM journey. All organizations are engaged in ERM practices at some level, but precious few have developed the risk management processes into a fully mature ERM program.

To be successful, an ERM program must be closely tied to the nature, scale and complexity of the risks being managed, hence, no two ERM programs will be identical. However, all successful ERM programs are built upon the foundation outlined above.

For more information contact Kevin Madigan at 518 • 288 • 0139 or [kmadigan@pinnacleactuararies.com](mailto:kmadigan@pinnacleactuararies.com)

Experience the Pinnacle Difference!