Article from
Risk Management
December 2017
Issue 40

ERM in Five Words

Part 1: Resilience, Transparency and Discipline

By David Ingram

Editor's note: "ERM in Five Words" will be published in a series of two articles. In this December issue, Part 1 illustrates the importance of Transparency and Discipline. Part 2, with a focus on Alignment and Adaptability will be published in the March issue of Risk Management.

Billy Joel sang that survival alone is a noble fight, but most companies want to do much better than just surviving. But the world is a dangerous and complex place. Surviving itself may be difficult, but the focus is most often on less extreme situations such as:

- Not making bonus
- Not beating last year
- Not beating competitors
- Not making a profit

In other words, a common goal that is informally set for risk managers is "no surprises."

Unfortunately, that goal forces risk managers to keep their focus on the small bumps in the road ahead. That may mean that there may not be anyone at all focused on the places where the entire road is washed out by a flood or blocked by an avalanche.

SURVIVING THE BIG CRISES REQUIRES RESILIENCE

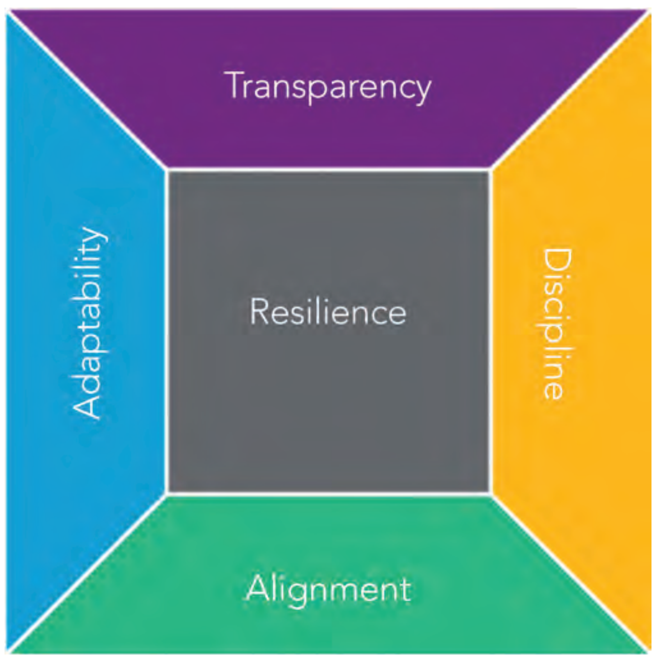
In the case of the really big disturbances, survival is the noble fight, and survival will often require resilience. As originally envisioned by the biologist C.S. Holling in 1976, resilience is achieved by constantly changing, renewing and reorganizing in order to survive, despite an extremely adverse situation. Resilience includes not just reactions to adversity, but the preparation for adversity, and the avoidance of adverse events and the worst effects of the disturbance.

Enterprise risk management (ERM) is the name for an approach to organizing risk management. I often describe ERM as a set of "n+1" control cycles, one for each of the "n" key risks and one more for control of the aggregate risk in comparison to the aggregate ability to absorb losses.

THE FOUR KEYS TO RESILIENCE

There are four key aspects of ERM that take it beyond "n+1" control cycles. The ERM process draws its power from transparency and **discipline**, and its direction from **alignment**, and can only maintain its effectiveness over the long term with adaptability. While each of the four keys to ERM provide these tangible benefits, resilience can only be achieved with all four.

1. **Transparency**—around level of exposures of key risks, the success or failure of risk mitigation activity and the gains or losses associated with risk exposures.
2. **Discipline**—the commitment to reliable management of all key risks and to the aggregate risk of the firm.
3. **Alignment**—consistency between the primary strategic objectives of the firm and the objectives of the risk management programs, so that ERM supports the primary goals of the firm.
4. **Adaptability**—planning to react to information about the changing risk environment to keep the focus on the risk management needed to succeed next year, not last year.



TRANSPARENCY

When banking regulators looked around at the financial institutions that fared less poorly during the financial crisis, one of the common themes that distinguished them was their dedication to internal transparency regarding their risks and risk management activities.

Risk management has been a part of business practices for thousands of years. ERM is a relatively new approach to risk management that, when taken to extremes, may noticeably increase the cost of doing business, and can take the attention of executives away from running their firms.

The executives in central roles at those firms had constant access to the best information available. Those banks tended to react faster when their aggregate level of risk looked like it was headed above their risk tolerance. They also seemed to get into less trouble with risk concentration caused by people in different parts of the firm unintentionally piling onto similar and likely highly correlated risks. Transparency is not expected from traditional risk management activities—business managers are taught to concentrate on sales and profits, with a third focus on expenses. Risk management is viewed as the fourth or lower priority of the business.

When Middle Managers Inherit Risk

Middle managers are most often charged with handling risk, and they get that responsibility sometimes as a (possibly private) inheritance from their predecessor. It may not even be included in their job description. Executive management may not know and seldom asks about risk as long as sales and profits are meeting expectations and expenses are within budget.

In those traditional risk management situations, the degree to which risk is tightly controlled or loosely allowed is often a personal decision made by the middle manager who inherited the responsibility for a particular risk. That person may make the best decision based on full knowledge of the nature of the risk and the availability and cost of mitigation of the risk, or they might just choose an approach based on poor or even inaccurate information because that is the best that they can find with the time they can spare.

ERM is a commitment to executive and board attention to the important risks of the firm. In a fully realized ERM program, the risk profile of the firm and the plans to change or maintain that profile from one year to the next—while exploiting, managing, limiting or avoiding various risks that are tied to their general business strategy—are shared among the management team and with the board.

In the best programs, it is not only shared, it is a topic of debate and challenge. These firms realize that a dollar of profit usually has the exact same value as a dollar of loss, so they conclude that risk management, well-chosen and executed, can be as important to success as marketing.

Transparency and Company Executive Management

Generally, executives are aware of the firm's risks, but until ERM comes along and forces an actual discussion of risk, there is rarely a spontaneous agreement on priorities. In a firm without ERM, the top executives would likely not even have the same list in mind for the company's top 10 risks. And different executives would have different Borel risk points.[1] With the transparency that comes from an ERM risk identification and prioritization exercise, the executives will come to agreement on the list of risks that will be the priority as well as the firm's agreed upon Borel point.

As risk transparency becomes common practice, management discussions can shift from simple risk avoidance and minimization to risk reward trade-offs and cost benefit alternatives of different risk mitigations. Management can also exploit the development of expertise in detecting and assessing shifts in the risk environment.

Transparency and the Board

Transparency of risk information is highly desirable to the board. While the details of a hundred risks are not necessary, they do want to know—before the next board—meeting that someone is attending to the risks that might end the company.

We usually recommend that management highlight five or six risks that are board-level concerns—the risks to the "enterprise." These most significant risks to the firm would all have the potential to cripple the enterprise either financially, operationally or reputationally.

Management would then regularly keep the board apprised as to:

- the level of exposure to these risks,
- the success or failure of risk mitigation activities and
- the gains or losses associated with these risk exposures.

These discussions of aggregate risk and the top enterprise risks should go through the normal management control cycle discussion of plans, execution, success or failure, reactions to changing conditions, and new plans.

Transparency and Staff

Transparency of risk information is important if a company wants to "get everyone involved" in risk management. For over 20 years, some companies have practiced open-book management (OBM), sharing detailed information about their financial statements and business plans. But financial statements rarely provide actionable information about risk. Therefore, even in the OBM firms, there is generally a lack of knowledge about risk. With the transparency of risk and risk management information that comes from ERM, risk communication can become a part of the "open book."

There may be a paternalist urge to protect employees from scary information about risk, but ERM provides a language for talking not just about bad things that can happen, but also about what is being done about it. By including more employees in the risk discussion, there is also an increased chance that the firm will become aware of critical changes in the risk environment and possibilities for enhancing mitigation activities to better achieve the firm objectives with less disruption from unexpected adverse events.

Transparency Outside the Firm

Few, if any, U.S. firms will actually publically describe their risk management activities. In the U.S., publically traded firms have long been required to disclose the company's risks in securities financial filings. But conventional wisdom holds that it is too risky to disclose anything about risk management. So, the reader of the financial statement is left wondering whether management is doing anything at all about the sometimes dozens of risks that are noted in the 10K. Other disclosures about very specific risk management activities such as hedging and reinsurance are included, but few, if any, U.S. firms will actually publically describe their risk management framework.

The story is completely different outside the U.S. With the development of ERM, large global insurers and reinsurers have been telling the story of their ERM programs for over 10 years. It is common for the largest non-U.S. insurers and reinsurers to disclose 10 to 40 pages of discussion of their risk management program. One reinsurer even discloses its risk limits and risk positions compared to those limits for a dozen major perils.

There also seems to be an emerging standard for insurers to provide a clear tabular exposition of their top risks, along with their main risk mitigation activities regarding each risk. These firms frequently have the Chief Risk Officer delivering presentations to investors, and joining the CEO and CFO in presenting quarterly financial results where the risk and capital position is considered to be one of the key financial results.

This transparency outside of the firm provides valuable information to investors who might be concerned with the risks retained by an insurer they invest in. Time will tell whether the insurers with better disclosure of risk management actually end up experiencing fewer or less severe losses and better return for risk retained.

DISCIPLINE

Risk management matters the most when it is the most expensive and most difficult. But unless the regular steps of risk management have already become muscle memory, it is much less likely that you will even think to do your risk management when times get tough.

ERM brings discipline to both the mitigation of individual risks and to aggregate risk management while also promoting a disciplined commitment to a comprehensive approach to risk management.

Disciplined Management of Individual Risks

Risk management is much like investing. Looking over the long term, a huge percentage of long-term gains come from being in the market for just a few days. The same is true for risk. The risk management benefits of limiting losses come in just a few quarters. Most of the time, risk management can be skipped without any harm being done. The harm comes when risk management is not already "on" when the lights go out.

It does not help at all to know after the fact when those good days for investing happened. And when "everybody knows" that

bad times are upon us, risk mitigation gets more expensive or even impossible. You will have a hard time buying insurance when the house next door is on fire or when the hurricane is racing up the coast.

To obtain the gains from investing, most investors need to consistently be in the market. And to get the benefits of risk management, companies need to practice it all of the time. Discipline is how you acquire the muscle memory to conduct the continuous risk management so that it is in place and ready to respond when the bad times finally come.

Making explicit plans for managing risk and then following up, checking on the execution of those plans, and reporting the results of those checks may seem like lots and lots of needless redundancy to some, but they miss the point. Discipline makes risk management reliable instead of being another wild card in an uncertain world and ERM brings this discipline to traditional risk management.

Traditional risk management (that is, pre-ERM risk management) is more ad hoc. Risk mitigation and control usually happens but there is typically not an explicit commitment to assuring that takes place.

Aggregate Risk Management

ERM also adds a new layer of discipline to risk management as it addresses the level of aggregate risk. The formation of a risk appetite and tolerance statement for a company itself imposes discipline on a conversation that previously, if it was addressed at all, was discussed in vague terms.

Clear and coherent communication is an often-underappreciated discipline that is much more difficult than it appears. ERM encourages insurers to clearly state their approach to risk as well as the amount and types of risks that they will accept and provides a script and outline that makes it easier to speak clearly about risk and risk management.

True discipline for aggregate risk management involves actually enforcing a control process for aggregate risk that is similar to the process of individual risks. This may involve management setting both

- a risk capital base (or limit), which the risk managers do not want the company to fall below under most circumstances, as well as
- a risk capital target, which is where they expect the relationship between aggregate risk and total actual surplus to end up.

Discipline involves not only setting these goals and limits, but also monitoring activities to track progress compared to said goals and limits.

It also requires making mid-course corrections when they are needed. In the rare situations where surplus is much closer to the limit than the goal, making the hard decisions about how the company must make serious changes to plans.

Comprehensiveness

Discipline is also needed to address the comprehensiveness of risk management. ERM includes the discipline of a commitment to addressing all of the significant risks of the firm and always starts with a risk identification and prioritization step, so that while all risks are considered, time and resources are used wisely by focusing only on the most significant risks.

> Risk management matters the most when it is the most expensive and most difficult.

Traditional risk management is also more ad hoc about which risks are addressed. People are not necessarily even asked whether they are paying attention to all of their risks. Sometimes the only risks that are addressed are the risks that the company is used to dealing with or the risks that have most recently affected the firm, other times it might be that just the risks that are convenient and easy to manage are addressed.

The emerging risks identification process within ERM brings a belt-and-suspenders approach to risk identification. Not only is there an explicit effort to identify all presenting risks, but with emerging risks management, there is a periodic effort to identify and prepare for future risks.

Transparency and Discipline are Keys

Transparency helps to enforce and encourage discipline. In a transparent organization, everyone will know if risk management stops or if there is a failure to maintain risk exposures within their established risk limits. Actual transparency is even better than guilt to hold people accountable to risk management, because transparency works even on those who are able to overcome their guilt in pursuit of riches.

Discipline is what makes risk management pay off. Without discipline, it is most likely that a company will incur the cost of performing risk management when times are good and losses from risks are light, but fail to consistently apply risk mitigations when risk is high and losses are large.

Transparency and discipline make ERM Strong. They are two of the keys to ERM.

The next two keys to ERM—alignment and adaptability, keep the ERM process on the right direction and maintain its effectiveness over the long term, will be discussed in part 2 of "ERM in Five Words" in the next issue. ■

David Ingram, FSA, MAAA, CERA, is executive vice president at Willis Re. He can be reached at *dave.ingram@willistowerswatson.com.*

ENDNOTE

1 The Borel Risk Point is the probability at which someone would choose to ignore a risk because it is too unlikely. One might have a one-in-10 year (90 percentile) Borel point because he is 10 years away from retirement. Another might have a one-in-50 year (98 percentile) Borel point because that is her guess of the rating agency sensitivity. A third a one-in-three (33.3 percentile) Borel point because that is the timeframe for the company's long-term incentive compensation.