

# UC Irvine

## UC Irvine Previously Published Works

### Title

Strategic Risk Management: A Better Way of Managing Major Risks

### Permalink

<https://escholarship.org/uc/item/6jt3b6mn>

### Authors

Bromiley, Philip

Rau, Devaki

### Publication Date

2016

Peer reviewed



## STRATEGIC RISK MANAGEMENT

# A Better Way of Managing Major Risks

By PHILIP BROMILEY and DEVAKI RAU

**F**ew companies invested more effort in risk management than Countrywide Financial. In 2007, the Institute of Internal Auditors praised Countrywide for its comprehensive enterprise risk management program, which involved 45 risk management professionals, supplemented by 112 internal auditors, assessing 530 risk matrices, 9,500 risks and 27,000 controls. “Countrywide’s program is truly best practice,” stated *Internal Auditor* magazine at the time.

A year after that glowing pronouncement, Countrywide was acquired by Bank of America in 2008, having essentially gone bankrupt due to unwise risk-taking in the subprime lending market. How could a company with such an

exhaustive system of risk identification, assessment and evaluation succumb to the very thing that it had gone to such lengths to avoid?

Our observations of risk-management practices point to a critical problem: managers often turn risk management into a massive paper-processing exercise. They become so busy identifying and evaluating every possible kind of risk facing their businesses that they miss the forest for the trees.

Instead, we believe that managers should focus on the risks that really matter – namely, strategic risks that threaten their firm’s existence. In this article, we suggest a different way to identify and manage risk, offering nine practical tips to help you manage your risks strategically.



Do firms want – or even need – to enumerate and evaluate each and every risk they could possibly face? Or do they just care about the big ones that might cause them to go bankrupt or face serious distress?

### Enterprise Risk Management: An Imperfect Science

Conventional wisdom on risk management suggests that firms manage their risks most effectively when they consider them as a portfolio. As portfolios generally have less risk than the underlying components, managing risks this way can result in lower risk-mitigation costs than managing risks individually.

For example, one business division might have a positive exposure to an exchange rate and another a negative, but taken together, the two could cancel each other out, leaving no corporate exposure to that exchange rate.

However, the risk of a portfolio depends critically on the correlations among the risks. Combining highly correlated risks offers little benefit in a portfolio, while combining uncorrelated risks can result in a portfolio risk far below the risk of its constituent parts.

This approach – termed Enterprise Risk Management or ERM – involves assessing all the risks facing a firm, classifying them by their probability and impact, and determining which actions to take to mitigate or control them. A firm might identify operational risks at the subsidiary level, the business unit level

and the division level. After identifying these risks, the firm would assess the likelihood and consequence of their occurrence. It would then identify how to respond to these risks in the context of the firm's internal environment, control systems, communication processes and so on.

Note that not all risks need to be treated as something to be mitigated or controlled. A firm with an advantage in addressing a specific kind of risk should explore ways to profit from that advantage.

Although attractive in principle, this approach has problems. First, ERM entails enormous effort. The job of identifying risks arising from firm operations at a variety of levels can be an immense undertaking.

Take the three-dimensional matrix or risk cube (see **Exhibit 1**) frequently used to depict the various interrelated levels of risk facing an enterprise. The eight main components of risk *times* the four categories of business objectives *times* the four business levels yield 128 different managerial considerations – and that's just for one kind of risk! Because there are so many enterprise risks, a firm can easily identify tens of thousands of potential risks, like Country-wide did.

And that's only the start. Next, managers need to assess the likelihood and consequence of those risks occurring. To handle these risks as a portfolio requires that managers know the distributions and correlations of the possible outcomes. Outside of financial investments, managers seldom have sufficient data for these estimates. Often, the most they can do is guess the likelihood of a risk occurring on, say, a scale of 1 to 5. The benefits of treating risks as a portfolio depend on the correlations among the underlying risks, yet managers seldom have legitimate data to estimate such correlations accurately or meaningfully.

Finally, managers should ask the same question about ERM that they would ask about

#### ■ EXECUTIVE SUMMARY

**In trying to identify all the risks a firm faces,** managers can turn risk management into an overwhelming paper-processing exercise that distracts them from focusing on the risks that really matter – namely, strategic ones that threaten the firm's existence. By not being able to grasp the assumptions and limitations of complex and costly Enterprise Risk Management (ERM) tools and models,

managers may be operating under a false sense of security. Based on their research on firm risk-taking and risk management, the authors offer nine practical suggestions to help managers make the risk function more meaningful and relevant. A healthy dose of skepticism, prudence and resilience will go a long way toward helping your firm see the forest rather than the trees.



any other business practice: what is the return on investment for this activity?

We have little evidence that ERM practices actually reduce risk, let alone justify the cost of implementing ERM practices. Any manager can take steps to reduce risk. But the real management challenge lies in judging the trade-offs between risk reduction vs. reduction in expected performance.

### Strategic Risks: A Different Approach

Given the inherent difficulty, if not impossibility, of ever fully identifying, assessing and evaluating all the risks that could ever have an impact on your business, we would argue that managers would do better to focus on strategic risks – those that pose the biggest threats to your company’s existence.

This shift of emphasis comes from an examination of what firms really want from risk management. Do firms want – or even need – to enumerate and evaluate each and every risk the firm could possibly face? Or do firms just care about the big risks – the ones that might cause the firm to go bankrupt or face serious distress?

Let us distinguish between strategic and operational risks. Put simply, managers must

address strategic risks because they threaten the performance or survival of the firm, whereas managers should address operational risks when doing so improves expected returns.

Take a banking example. On the one hand, a bank need not be overly afraid of the risk per se associated with small loans (an operational risk) – though it should be concerned that the interest rate charged is sufficient that the loan has positive expected returns. On the other hand, the bank should worry about the overall risk of its loan portfolio or its trading activities because either of those constitutes a strategic risk that could kill the bank.

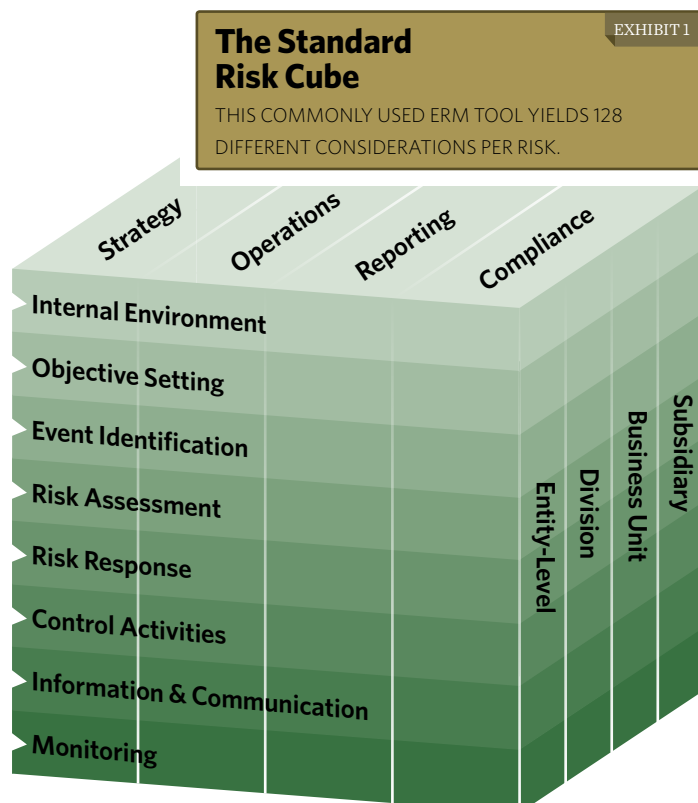
Likewise, in a production environment, the defect rate is a form of operational risk that should be managed when it pays to do so, but major product liability issues are strategic risks that could seriously damage the company.

Most firms really want risk management to help the firm avoid crises that threaten its survival. However, barring regulators and consultants, risk management is probably not the single most urgent or pressing concern weighing on managers’ minds. Profits probably matter more, since profits are real while risks are only estimates.

Moreover, the central ideas underlying the concept of risk are rather slippery. For example, how does one define “risk”? Is it the size of potential loss, the probability of potential loss or some combination of the two? Do your risk estimates depend on historical data (assuming such data exist) or the gut feelings of your managers? If your risk estimates depend heavily on managerial judgment, they will almost always be biased.

Forecasting is a case in point (after all, a risk assessment is essentially a forecast of risk). While forecasting can be quite accurate in well-understood, repeatable environments, it can be quite problematic in novel or less understood domains. The track record for new product introductions suggests that 9 out of 10 fail, but 10 out of 10 were predicted to succeed. Likewise, most observers estimate that 5 out of 10 corporate acquisitions fail, when again 10 out of 10 were predicted to succeed, at least by the managers who made those decisions.

There is no reason to believe that managers are better at estimating risks than they are at forecasting other non-repeated items like these. Even ignoring the distorting effect of





Even if your firm could collect accurate data, free from any bias, you would still face the problem of what to do with such information. Few managers have the expertise and competence to estimate risk from these data.

incentives and organization-specific issues, research on behavioral decision theory consistently demonstrates that people, including professional analysts, are terrible intuitive statisticians. Depending on extraneous factors, they systematically over- or underestimate the likelihood that a particular outcome will occur.

Even if your firm could collect relatively accurate data, free from any managerial bias, you would still face the problem of what to do with such information. Few managers have the technical expertise and competence required to identify and use the right tools to estimate risk from these data.

Given that managing risk has both direct costs (in forgone earnings) and indirect costs (in managerial time), executives need to think long and hard about how much risk management they need. Rather than trying to identify and manage a host of risks, you may be better off focusing on the strategic ones that could potentially sink your firm (see **Exhibit 2**). Here we offer nine tips to help you do that.

#### ■ ABOUT THE AUTHORS

**Philip Bromiley** is the Dean's Professor in Strategic Management at the Merage School of Business of the University of California, Irvine. He is the former Curtis L. Carlson Chair in Strategic Management and chair of the Strategic Management Department at the University of Minnesota's Carlson School of Management. He is the author of over 70 journal articles and book chapters as well as two books, *Behavioral Foundations*

*of Strategic Management and Corporate Capital Investment: A Behavioral Approach.*

**Devaki Rau** is an associate professor in the Department of Management at Northern Illinois University's College of Business. She previously worked in the Indian software industry. Her research interests are organizational learning, strategic decision-making and top management teams.

#### 1 RECOGNIZE WHERE THE REAL PROBLEM LIES

Sometimes the problem is not risk management but *management*. Many observers attribute the recent financial crisis to inadequate risk management by banks and other financial institutions. In some cases, however, the problem was not risk management per se but management decisions that ignored or overruled warnings from the risk management function.

As previously mentioned, Countrywide had an extremely sophisticated risk management system. But it was Countrywide's *management* who publicly stated that the company would match any loan made by a competitor.

The same goes for New Century Financial, another big provider of subprime mortgages in the United States. In their article "New Century Financial: Lessons Learned," Michael J. Missal and Lisa M. Richman note that it wasn't that the risks weren't being detected: they were. "In fact, a number of board members were openly disdainful of certain members of senior management, and challenged their integrity and competence." The "unhealthy friction" between the board and senior management "inhibited an open flow of information ... and restricted the ability of New Century to react nimbly and effectively to the rapidly deteriorating subprime market." Internal auditors at New Century repeatedly objected to the riskiness of the loans being made, but management did not respond.

#### 2 BE SKEPTICAL OF SOPHISTICATED RISK MODELS

Wall Street banks, among the most sophisticated risk managers in the world, led us into the 2008 recession. These banks may have taken too many risks with subprime mortgages precisely because they relied on sophisticated risk-management systems that used formal, extremely elaborate models. These models gave managers an unjustified sense of security



Sophisticated models may appear to make uncertainty magically disappear – particularly when the managers who use them gloss over or view with unquestioning reverence the details of the underlying analyses.

**Not All Risks Are Equal**

EXHIBIT 2

THIS IS A LIST OF 50 RISKS IDENTIFIED BY ONE CONSULTANT. THE REAL QUESTION IS: WHICH OF THESE ARE THE STRATEGIC ONES FOR YOU?

Strategic Risks	Operational Risks	Financial Risks
<ul style="list-style-type: none"> <li>■ Industry</li> <li>■ Economy</li> <li>■ Political Change</li> <li>■ Competitors</li> <li>■ Consumer Preference</li> <li>■ Market Share</li> <li>■ Reputation</li> <li>■ Brand Equity</li> <li>■ Strategic Focus</li> <li>■ Investor Confidence</li> </ul>	<ul style="list-style-type: none"> <li>■ Customer Satisfaction</li> <li>■ Product Failure</li> <li>■ Supply Chain</li> <li>■ Sourcing</li> <li>■ Supplier Concentration</li> <li>■ Outsourcing</li> <li>■ Election Cycle</li> <li>■ Catastrophic Loss</li> <li>■ Process Execution</li> <li>■ Policies and Procedures</li> <li>■ Environmental</li> <li>■ Contract</li> <li>■ Regulatory and Legal</li> <li>■ Human Resources</li> <li>■ Health and Safety</li> <li>■ Authority</li> <li>■ Integrity</li> <li>■ Leadership and Empowerment</li> <li>■ Culture</li> <li>■ Performance Incentives</li> <li>■ Knowledge Capital</li> </ul>	<ul style="list-style-type: none"> <li>■ Cash Flow</li> <li>■ Liquidity</li> <li>■ Availability</li> <li>■ Interest Rates</li> <li>■ Foreign Exchange Rates</li> <li>■ Credit Capacity</li> <li>■ Credit Concentration</li> <li>■ Credit Default</li> <li>■ Accounting</li> <li>■ Budgeting</li> <li>■ Taxation</li> <li>■ Pricing</li> <li>■ Performance Measurement</li> <li>■ Portfolio</li> <li>■ Systems Infrastructure</li> <li>■ Systems Access</li> <li>■ Systems Availability</li> <li>■ Data Integrity</li> <li>■ Data Relevance</li> </ul>

about their risk assessments.

Sophisticated models may appear to make uncertainty magically disappear – particularly when the managers who use them gloss over or view with unquestioning reverence the details of the underlying analyses. Indeed, Wall Street banks and investment firms were hiring rocket scientists and similarly trained individuals who, with a very limited understanding of the lending system, produced risk

models that the average manager had little chance of understanding.

Here's a simple example: Suppose you make 10,000 products with a 5 percent chance of defects. Or you give out 10,000 loans with a 5 percent chance of default. Obviously, you would expect 500 defects or defaults on average, but how likely is it that you would encounter 600 or more defects or defaults?

If the defects or defaults are randomly distributed, the answer is .00045 percent. In other words, if you assume a 5 percent defect rate or default probability, your models will assure you that the chance of you seeing 600 defects or defaults is virtually nil.

However, this analysis rests heavily on an assumed defect rate of 5 percent. If you err a little in predicting the defect rate, and the true defect rate is 6 percent, then 600 moves from impossible to the most likely outcome.

A similar problem occurs with independence. If borrowers default on loans randomly, then the estimate holds. But if these were home loans and some defaults lower the value of houses, thereby triggering more defaults as individuals with financial troubles can no longer sell their homes, then defaults are not independent. Likewise, if machines make defects randomly, we have a good estimate, but if one malfunctioning machine results in many defects, then defects are correlated.

Few managers have the technical ability or time to evaluate risk-assessment models in depth. As a poor substitute, they should at least be skeptical.

**3 BEWARE OF INCREASING RISK FOR PROFIT**

One of the major problems with strategic risks is that they occur infrequently. If they didn't, we would see a high percentage of firms going bankrupt every year. We have great difficulty estimating the probabilities of infrequent events.



The point is not to develop detailed plans for every scenario, but to highlight major environmental risks in general, so that you can at least accommodate them in your strategic planning.

How does this matter for organizations? Consider a manager making decisions. If the outcomes of his or her decisions are positive (or at least nothing goes wrong), the manager might see no harm in taking more risks the next time. At an organizational level, markets might push firms into increasing amounts of risk, eventually making them take on as much risk as their peers, just to stay in business. Incrementally, the manager or firm can increase risk to undesirable levels.

In a safety example, NASA launches had indicators of design problems but nothing went really wrong. Consequently, the organization kept taking risks – until a manned mission exploded.

In a banking example, before the crash, if a mortgage lender was not as generous as the most generous competitor in the market, the lender did not make loans. Each time a lender became more generous – by lowering underwriting standards or increasing the loan to house value – competitors were forced to match. If they didn't, they were essentially out of business.

Before the crash, lenders made winking references to “liar loans” (based on stated income) and “NINJA loans” (No Income, No Job or Assets) but a company that did not issue these had difficulty staying in the market. Such creeping risk could occur in a variety of domains – from ancillary commitments to product warranties to product quality, where quality is not immediately evident to the buyer.

#### 4 TRY SCENARIOS

One approach to identify strategic risks is scenario analysis. You start by identifying a few key variables on which there is uncertainty. Then, you develop logically consistent scenarios based on the different values of these key variables, and evaluate the major

uncertainties in each case. Oil companies do this to anticipate the impact of drastically different oil prices: what happens if crude is \$50, \$100 or \$150 per barrel?

If you use scenarios to assess strategic risks, be aware of the general tendency to underestimate the variability. In July 2014, when crude cost \$110 a barrel, few would have given it much chance to be \$30 a barrel by January 2016, but this happened.

The point is not to develop detailed plans for every scenario, but to highlight major environmental risks in general, so that you can at least accommodate them in your strategic planning.

#### 5 HOLD PREMORTEMS

In most companies, naysayers aren't welcome. People prefer can-do managers. If the senior management team leans toward X, rare is the person who will stick his head above the parapet to voice arguments against X. And if X turns out to be wrong, no one likes the person who says, “I told you so.”

Writing in *Harvard Business Review*, Gary Klein proposes an alternative form of expressing concerns without becoming the smug Monday-morning quarterback. The opposite of a postmortem – in which problems are dissected *after* they've occurred, when hindsight is always 20/20 – Klein's premortem technique encourages people to point out all the ways that things could go wrong *before* any action is taken.

Under this “prospective hindsight approach,” everyone assumes the failure of whatever is being proposed, and they spend their time developing potential reasons for that failure. With such reasons identified, managers can strengthen the plan. The premortem helps overcome the tendency of managers always looking on the bright side.



Apart from excessive risk-taking, ill-conceived incentives can provoke the opposite problem: risk aversion. Managers will likely not take too many risks – even risks the company might want to take.

#### 6 USE EXTERNAL COMPARISONS

Most risk analyses focus on the issue at hand and attempt to predict the future outcomes for that particular issue. However, such predictions often have systemic biases. Most of us are familiar with the tendency to underestimate how long tasks will take and how much they will cost. Much of this comes from estimating the *minimum* expected time, if everything goes according to plan, and not the *actual* expected time.

Managers can combat this tendency by using a comparable reference group. In estimating how long a project should take, create a list of roughly similar projects and look at how long they took. In estimating costs, do the same thing. These comparisons do not even have to be terribly close. Then you can adjust from your normal prediction, recognizing how long similar things have historically taken and how much they have cost.

#### 7 PAY ATTENTION TO INCENTIVES

Risks in general, and strategic risks in particular, stem from managerial decisions that depend heavily on incentives. While incentives have clear benefits, sometimes they work too well, especially when they are strong and the risk associated with the action is unmeasured or unmonitored.

Securities trading is a prime example. Successful risk-taking can result in hefty bonuses for individual traders, while the company bears the losses associated with unsuccessful risk-taking. An employee who has lost enough to end his or her career may take excessive risks, believing he or she has nothing to lose. Several banks have been destroyed by individuals doubling-down on small losses to create catastrophes.

Apart from excessive risk-taking, ill-conceived incentives can provoke the opposite

problem: risk aversion. In most companies, the middle manager who takes a big risk that pays off may get a nice bonus and perhaps a promotion, but if it turns out badly, he or she may get fired. With that kind of reward system, sensible managers will likely not take too many risks – even risks the company might want to take.

#### 8 DON'T FORCE GROWTH

Sometimes strategic risks stem from a company in a traditional industry setting extremely aggressive growth targets, based not on sound business logic but on arbitrary ambition. To meet these targets, the firm may pursue acquisitions or other actions that increase its strategic risks.

In their paper “Just Say No to Wall Street: Putting a Stop to the Earnings Game,” Joseph Fuller and Michael C. Jensen document the case of Nortel Networks, which between 1997 and 2001 paid over \$32 billion to acquire 19 companies in an attempt to satisfy analysts’ growth expectations. The telecom company’s strategy was to transform itself from voice transmission to data networking, but it overextended itself, fueled by heady market valuations. In the end, most of those acquired companies were sold, shut down or written off. Nortel’s stock nosedived, it hemorrhaged staff and by 2009, the company had gone bankrupt.

#### 9 BUILD A RESILIENT ORGANIZATION

Most organizations face an untold number of low-probability, high-impact events. Their low probabilities make identification and management of each potential event uneconomic and infeasible. That said, given the large numbers of these potential events, the odds of one of them occurring are quite high.

Instead of managing all these events, firms must build a capability to respond to unanticipated events. In other words, they must build





To build a resilient organization, try to keep some resources in reserve. In addition, have systems that acknowledge and adapt to problems rather than hiding them. This implies a culture of transparency.

a capacity for *organizational resilience*. Managers will always face surprises. Instead of trying to anticipate all the low-probability but high-impact potential surprises, managers should focus on building systems and processes that allow their firms to recover quickly from them.

A legendary tale in this regard is the time when lightning struck a Philips plant in March 2000, causing a damaging fire that interrupted the supply of chips for Ericsson and Nokia cellphones. Though both Nokia and Ericsson estimated a one-week delay in chip deliveries, Nokia went further, holding daily discussions with Philips engineers. In doing so, Nokia discovered that a week was an underestimate, and it quickly sought alternative suppliers. By the time Ericsson cottoned on, Nokia had locked up most of the alternative suppliers. The end-of-year results spoke for themselves: Ericsson reported losses, blaming component shortages, while Nokia increased its handset market share, thanks to quick thinking in the face of a freak event.

To build a resilient organization, try to keep some resources in reserve. Being too fat is not good, but neither is having no fat. In addition, have systems that acknowledge and adapt to problems rather than hiding them. This implies a culture of transparency, so that covering up problems becomes difficult. Rather than scapegoating, firms need a culture where people feel free to admit mistakes with minimal fear of being penalized. Decentralization also allows adaptation to problems as and when they occur.

### Draw on Past Experiences

Throughout this discussion, it's important to remember that while risks – strategic or otherwise – can be predicted (to some extent) and managed (also to some extent), they are risks precisely because they cannot be completely anticipated or controlled. Perhaps the biggest takeaway from this article is that we can never

completely eliminate risk – but we can build adaptability and resilience into our organizations and management systems.

As a final thought, remember that if your firm is in business today, it has survived the worst recession since the Great Depression. In other words, your firm has survived the 70-year storm. Rushing to reduce future risks based on experience in the 2008 global financial crisis could easily result in overreaction – an example of locking the barn door after the horse has bolted. Indeed, if your firm did not experience difficulties in the recession, it probably was not taking enough risk. Instead of rushing into a massive risk-management exercise, try to target your risk management activities to emphasize the strategic issues that will determine organizational survival. □

### ■ TO KNOW MORE

- Bromiley, P. and D. Rau. "Looking Under the Lamppost? A Research Agenda for Increasing Enterprise Risk Management's Usefulness to Practitioners." In *Contemporary Challenges in Risk Management: Dealing with Risk, Uncertainty and the Unknown*, edited by Torben Juul Andersen, 50-62. Palgrave Macmillan, 2014.