SOCIETY OF ACTUARIES

Article from:

The Actuary Magazine

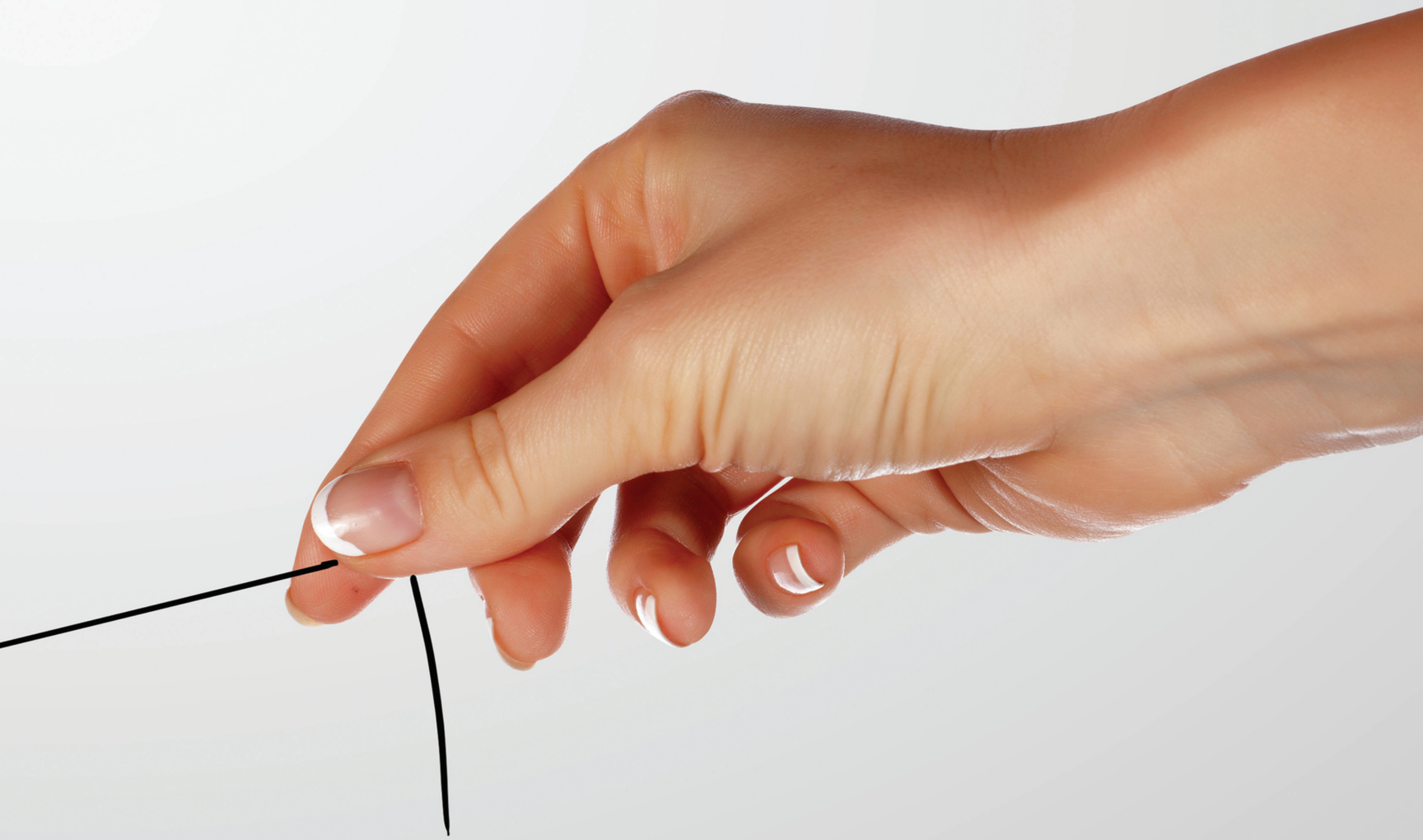
June/July – Volume 12, Issue 3

OPERATIONAL R

AND WHAT DO

ISK—WHAT IS IT?

I DO ABOUT IT?



It's time to get really serious about monitoring, measuring and managing the increasingly important operational and business risks that have been with us for many years as economic risks. By Larry Zimpleman

A robust enterprise risk management (ERM) program is at the heart of managing any financial services company—bank, insurance company, etc. Over the years, we have developed increasingly sophisticated ways of measuring and managing economic risks —equity market risk, interest rate risk, foreign currency risk, credit risk, etc. We now have an annual process whereby the Federal Reserve releases the results of its "stress tests" to see if our largest banks have a sufficient level of capital to withstand the next financial crisis.

But when you look at actual events that have gotten financial services companies in trouble, the risks mentioned above are not necessarily the drivers. It might be a rogue trader, it might be a DDOS attack by cybercriminals or a nation-state like North Korea, or it might be a compliance issue with a fine measured in billions. There is increasing recognition by many parties—regulators, boards of directors and even customers—that in the post-financial-crisis world there needs to be an increased emphasis on risks that go well beyond just economic risks.

So, how should we think about *those* risks and, more importantly, how can we measure, monitor and manage those risks?

OPERATIONAL	BUSINESS
Fraud (internal or external)	Conduct and ethics
Damage to physical assets	Reputation
Supplier and vendor management	Legislative and regulatory change
Employment practice and workforce safety	Accounting change
Business disruption and system failures	Branding/marketing
	Distribution/sales

All of these newer risks fall into a broad category of risks that we might label as "operational risks," or, perhaps even better, "operational and business risks." To be clear, these operational and business risks are *not* unique to financial services companies. Operational and business risks impact all businesses. But, since financial services companies' success is tied to their reputation and trustworthiness, operational and business risks are *just as important*—or maybe more so—than economic risks.

Even though operational and business risks have been with us for as many years as economic risks, it's only in the past few years—and especially since the financial crisis—that we've really started to focus on these risks and have begun to get serious about how we can monitor, measure and manage these increasingly important risks.

Fortunately, many of the same methodologies that we have used for the last 20 to 30 years to handle economic risks can be adopted to work for operational and business risks. This is why actuaries involved in risk management must expand their thinking and their horizons to include operational risk if their aim is to provide a comprehensive view of ERM.

1. First, we need to have a clear definition of our operational and business risks.
2. We need to have an understanding or profile of these risks to know the potential importance of each and how that risk is trending.
3. We need to have a "risk dashboard" to monitor on an ongoing basis how each operational risk is evolving. This is done by having key risk indicators for each risk as well as a "risk appetite" that helps to define the overall level of risk we choose to take. After all, risk is a necessary part of doing business and we can't eliminate all risk.
4. Finally, we need a risk improvement plan if some of the operational and business risks are outside of our risk appetite.

So, how should we think about those risks and, more importantly, how can we measure, monitor and manage those risks?

RISK CATEGORY	UNDERLYING RISK	RISK TREND
Fraud	High	↑
Damage to physical assets	Moderate	↔
Supplier/vendor management	High	↔
Business disruption	High	↑
Reputation	High	↑
Legislative/regulatory change	Moderate	↑
Branding/marketing	Moderate	↔

Before I go into more detail on the steps, I'd like to offer a few general comments on operational and business risks:

1. The nature of these risks says they are more difficult to measure or quantify—but that should not stop us from trying.
2. Many of these operational and business risks arise from your interactions with your customers and suppliers. One critical component in mitigating operational risk is to have a clear statement of core values of your company—how you want to do business. And you need to communicate again and again those core values to new and existing employees so your expectations are clear.
3. These risks are getting increasing attention by both boards and senior management. Does each position description for employees have a clear statement on adherence to core values? Is it part of the evaluation of senior management compensation?

Let's start with a listing of some of the major operational and business risks (see page 34):

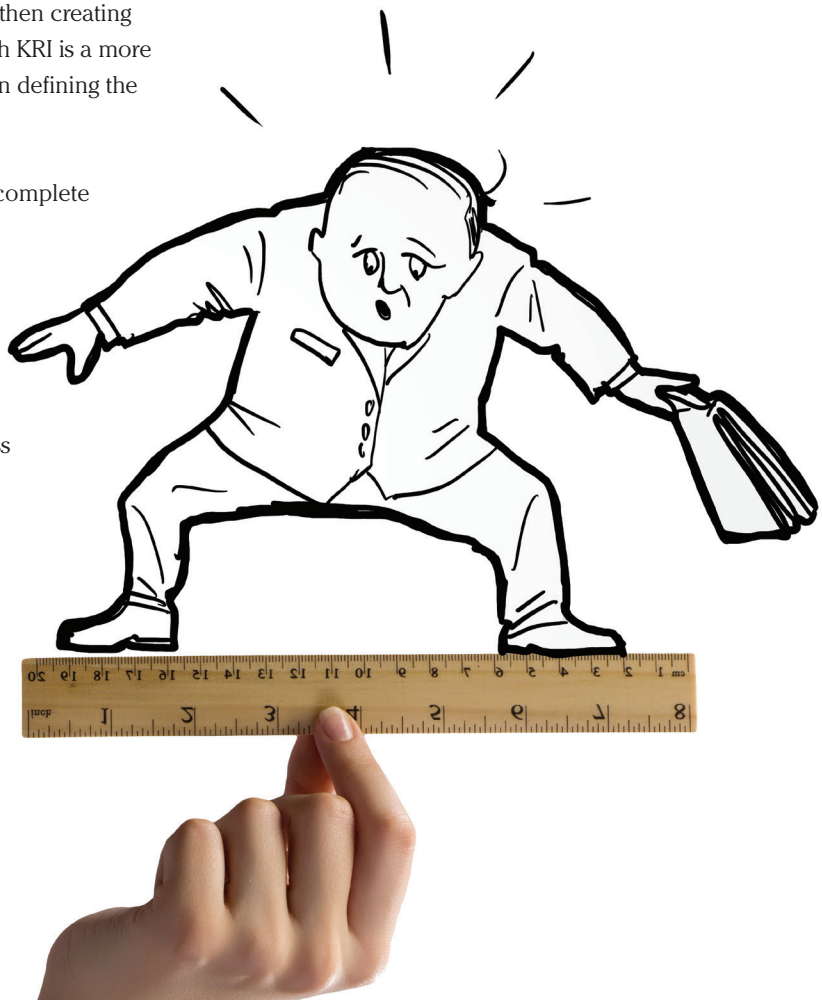
Each company may have some different risks under each category and the priorities may differ. But, overall, the list should clearly include all of the major functions of the company.

While defining the operational and business risks of your company is not easy, I find that the task of developing key risk indicators (KRIs) for each risk and then creating proper measures for each KRI is a more time-consuming task than defining the risks.

I won't try to provide a complete testing of KRIs for each operational or business risk, but Appendix A at the end of the article gives some examples of KRIs for several of the operational and business risks mentioned earlier.

A few points on KRIs:

1. You will want to evaluate each KRI regularly to be sure it is appropriate.
2. Though difficult, you should try to create as many quantifiable KRIs as you can.
3. A single KRI could measure more than one operational or business risk.
4. For the quantitative KRIs, don't set the bar so low that it becomes automatic that you will pass the KRI. You should expect that, in any single year, you



would see 15 to 20 percent of the KRIs that are outside of the tolerance you expect. This is how you can prioritize and improve your company performance.

Now that we have defined each operational and business risk and we have one to five KRIs for each of the risk categories, we are ready to begin to bring all of this information together in a consistent and organized way so it can be used to inform both senior management and the board of your operational and business risks.

First, we create a "risk profile assessment" for each operational and business risk. This assessment is admittedly subjective. The purpose of the assessment is to help the reader understand:

1. The underlying risk of each risk category, and
2. The trend in that risk category (increasing, stable, decreasing).

Let me provide a simplified model of the risk profile assessment (see page 35):

While this is a fair bit of subjectivity in the risk classification, it still provides a relative picture for the board and senior management of which are the most important operational and business risks and how are they trending. That relatively simple dashboard can then shape more discussion into the areas of greatest interest. This sort of tool is also excellent to use with regulators and rating agencies so they can more effectively see the internal processes you have in place around these important risks.

While each company will be different with respect to its exposure to operational risk, some of the more significant operational risks today are:

1. Supplier and vendor management: What standards are in place for who you do business with? Does a local supplier offer a "back door" entry point for a cyber thief who wants to get to you?
2. Business disruption: While most companies today have business continuity exercises, are they complete enough? We saw this firsthand at Principal in 1993 when a flood wiped out our local water works, leaving us without water for eight days. That impacts computers, servers and even your ability to occupy higher floors as your sprinkler systems will not function.
3. Legislative and regulatory change: Does your management team spend enough time on this important topic? Could tax reform and a changed set of tax incentives cause a significant disruption to your businesses?

The final piece of the risk management puzzle is to have an overall plan for improving the oversight and management of these business and operational risks. Elements of the program should include:

1. Discussion and agreement on which risks need to be the priorities for improvement—i.e., which risks are outside the company's risk appetite? What is the plan for bringing those risks back inside the desired tolerance?
2. Continued work to further define and change, when necessary, the risk definitions. One tool that can help with this is to have a "risk library" that is used across the company. This can be especially important in global organizations where language and cultural differences can be an impediment to clear and consistent understanding.
3. The nature of a maturing risk management system is that it will begin with mostly qualitative measures. The goal should be to improve to more quantitative measures over time. These are areas like fraud and damage to physical assets where quantitative measures are easier, although most companies do not aggregate this information regularly.
4. Transparency of results is key—both up to senior management and the board as well as sharing results with each of the business units for discussion and refinement.
5. Finally, think about how your operational and business risks are impacted over time by real-world events both inside and outside your company. Clearly, cyber risk is increasing for all companies. Have you started new businesses? Have you opened new offices or started business in new countries? Have you done recent acquisitions? If you have, did you do a comprehensive due diligence on operational risk? History shows that a more acquisitive strategy increases operational risk. Are there new teams running your businesses? All of these can have a real impact on the aggregate operational and business risks of your company.

While I hope this discussion has been helpful in thinking about how to approach the measurement and monitoring of operational and business risks, the most important thing to remember is that this is a journey—you can always improve your understanding of these risks and your measure of these risks. New risks will get added. It's doubtful that any will go away. But just as "hope is not a strategy," operational and business risks will not go away by not thinking about them or not trying to monitor them. Once boards, executives and risk management professionals begin to monitor and measure risk, you can take greater control of your future and reduce the odds that your company will be in tomorrow's headlines. A

Larry Zimpleman, FSA, MAAA, is chairman and CEO at Principal Financial Group, in Des Moines, Iowa. He can be reached at *larryzimpleman@principal.com.*

APPENDIX A

OPERATIONAL RISK	POSSIBLE KRI
Fraud	Code of ethics completion Unauthorized transactions Whistleblower calls/reports
Vendor management	% compliance with standards
Employment practices	Succession plans in place High-performing retention rate
Business disruption	System availability % Business continuity testing results

BUSINESS RISK	POSSIBLE KRI
Conduct and ethics	% verifying reading of code of ethics Number of customer complaints Regulatory inquiries
Reputation	Media monitoring results
Regulatory and business practices	Complaint tracking Suspicious activity reports
Branding/marketing	Brand power measures Loyalty measures