Taking a More Direct Road to Reducing Operational Risk

Ilya Sobko/Shutterstock

••The authors advocate a simpler approach with clear levers for fixing operational problems and delivering several types of value to the business.

BY GABRIEL DAVID AND BRIAN BARNIER

As the discipline of operational risk management continues to evolve, the following questions routinely surface among practitioners and senior management:

- "I know that risk and performance convergence is a good idea, but how do we make the linkage easier and meaningful?"
- "How does ops risk management add value?"
- "How do we know which business improvements will best reduce ops risk capital?"
- "How do we account for reductions in ops risk capital due to root-cause fixes and business process improvements?"

Challenges in Operational Risk

Over the past few years, national banking regulations and Basel II have drawn attention to operational risk. The main operational risk management outputs have been control catalogs, key risk indicator (KRI) reports, risk and control self-assessments (RCSAs), and capital calculations. While these outputs are usually helpful to varying degrees, operational risk managers are still looking to attain the next level.

Because financial institutions today are more dependent on information technology and infrastructure, quality control processes have become more useful.

In addition, operational risk managers must confront the harsh impact that operational risk has on bank earnings. A recent paper completed by a subgroup of the Basel Committee on Banking Supervision outlines operational risk's effects on a bank's income, with estimates based on calculations for operational risk capital as a percentage of gross income. These estimates range from 11.6% of gross income for Basel II AMA (advanced measurement approaches) banks to 13.1% for non-AMA banks in North America. Comparable figures elsewhere are 10.7% to 12.1% in Europe; 12.4% to 14.6% in Japan; and 7.8% to 13.9% in Australia.[1] While the analysis applied to larger institutions, the logic holds for even the smallest banks.

The key point is this: Operational risk managers can apply lessons learned in industrial business processes and quality improvement to reduce risk, thereby lowering costs, improving customer satisfaction, and increasing flexibility to drive new revenue.[2]

Back to the Future

Operational risk management is not new. When Basel II was being discussed in the period from 1997 to 2008, the Basel Committee on Banking Supervision and the Committee on the Global Financial System sought guidance from other industries' approaches to risk management and quality improvement.

A 2003 paper stated that "in the final analysis, Basel II is about the full industrialization of the global financial industry (banking in particular); realigning a bank's activities and businesses based on the best risk-adjusted return on capital and re-engineering the complete supply chain at least cost, least risk and best quality."[3] In essence, the failure of processes and controls causes operational risk and related losses.

Because financial institutions today are more dependent on information technology and infrastructure, quality control processes have become more useful—not only to cut costs, but also to reduce operational risk and the resulting capital.

Industrial methods can be used in financial services to create a more direct link between operational process and capital requirements. Among the many benefits are:

- Improved controls and accuracy.
- Ability to focus on gaps in detecting problems (both control and environmental threats).
- Greater ability to understand different types of threats.

Three Steps to Reducing Operational Risk

To benefit from these industrial approaches, institutions should make the approach straightforward in order to achieve the necessary clarity that makes it easier to take action. Institutions that leverage existing business process and quality improvement initiatives will be better prepared to implement these approaches.

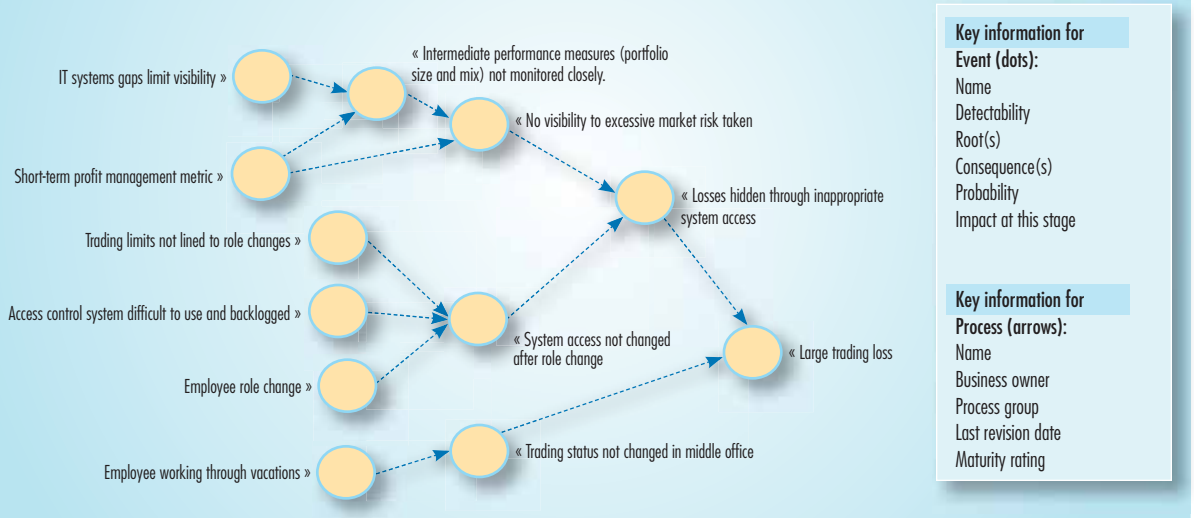
1. Understand the business.

- Gain a shared understanding of how the business works from the perspective of the various groups: business line, functional, and operational risk. This understanding includes 1) the business processes' end-to-end descriptions, and 2) the dependencies of those processes on information technology, integration, and other enablers. Automation and integration are important to improve consistency, accuracy, and speed and to understand what could go wrong in IT to hurt the business.[4] *Tip:* To assess business value, understand customer touch points in the revenue-generating processes. Here, you'll find operational risks to revenue that grab the attention of business leaders (not just compliance issues that are seen as just adding cost without value).
- Describe variations from the documented processes and the controls in the processes. These include variations due to error, innocent expediting (which can cause problems), and formal exceptions. The point is to understand what happens, good or bad, when the process is not followed. A higher percentage of exceptions (formal and informal) is a flag indicating the need to fix the core process. *Tip:* Smaller institutions should look for fast payback activities, such as converting from manual to automated controls.
- Determine your ability to detect control and environmental-threat problems and to see root-cause events. A variety of well-established tools can help you both avoid the "head in the sand" syndrome and see in "dark corners." These tools include fishbone diagrams, project management activity flow charts, and dependency maps, encompassing people, processes, and technology. The maps should clearly illustrate how root-cause events roll into consequent events. Events happen in chains. Nothing is a singular, simply because real life is an unfolding chain of events. The "space shuttle exploded" is not the only event. There were many events that took place before and after it. The point is to find the O-ring and the process that would have avoided the explosion before the explosion. The subprime mess is

Figure 1

Simple Event-Flow Diagram and Key Descriptive Information

The different flows illustrate three basic ways for events to unfold: cascading, coincidental, and direct.



a very long chain of cascading failures. Importantly, this step helps avoid the trap of confusing consequences with threats or causes.

Deliverables: End-to-end business process maps (including existing controls), diagrams of dependencies on automation and integration, lists of root causes, and detection gaps (which can be as simple as a red dot on a process diagram to show where problems are difficult to detect).

2. *Understand the risk to desired business outcomes (share value, profit, or customer satisfaction).*

- To understand scenarios that can disrupt the expected outcomes of business processes, begin by looking at control failures. This article describes scenarios that are more robust than typical "tail testing." They apply to a range of threats and event magnitudes. They include both cascading (looking at conditional probabilities) and coincidental impacts. For example, to state "fluid loss in the car results in failure" is not sufficient. A more robust scenario would describe a lack of washer fluid, mud space on the windshield, and then a crash. This provides a chain of events and makes it distinct from other fluids such as oil.

In financial services, a similarly limited scenario would be "server goes down, delaying mortgage-processing time." A more robust scenario would examine economic conditions and determine if the bank has visibility in the end-to-end business-IT process—from mortgage broker to investment bank—to uncover any problems and take action to reduce loss. IT provides the key information to avoid failure and loss, just as it provides crucial information in solving crimes or running industrial supply chains.

Another limited scenario is, "How long does it take to get server xyz up after it fails?" A more robust version would be, "How long does it take to resume supplying cash through ATMs if server xyz goes down during a regional blizzard due to part failure?" Similarly, a scenario of "$50M loss due to litigation xyz" is inadequate. Rather, a more complete scenario is "Product launch without full knowledge of state-specific variations in regulation, combined with inadequate training of new employees following acquisition, leads to compliance gaps, customer claims liability, and protracted negative publicity."

So that you can propose solid business cases for improvements that reflect real operations, it's important to capture both the big and the many daily losses that add up from root-cause events. A best practice is to use scenario analysis workshops that deeply engage business line, product owner, and functional leaders. A good workshop should be both sobering and engaging, leading to comments such as "This was fun" and "We should have done this long ago."[5]

- Determine the frequency of root-cause events by analyzing how events unfold and how smaller events snowball into larger combined events. By definition, root-cause events occur more frequently than do resulting or consequent events. The ratio of the former to the latter can be 100 (or more) to 1. *Tip:* The information is easier to understand and more powerful when presented as annotations to the dependency diagrams, process flows, and other visuals discussed above. Figure 1 shows a simple example.
- Understand the impact of risk (including cascading impacts and consequences to understand the full effect). The key is to include the range of impacts and consequences.

Adopting a New Approach to Operational Risk

FAQs from Ops Risk Managers

Q Won't this approach slow down our ops risk management process? Previously, we just focused on the spreadsheet. Now we need to spend time documenting the business processes.

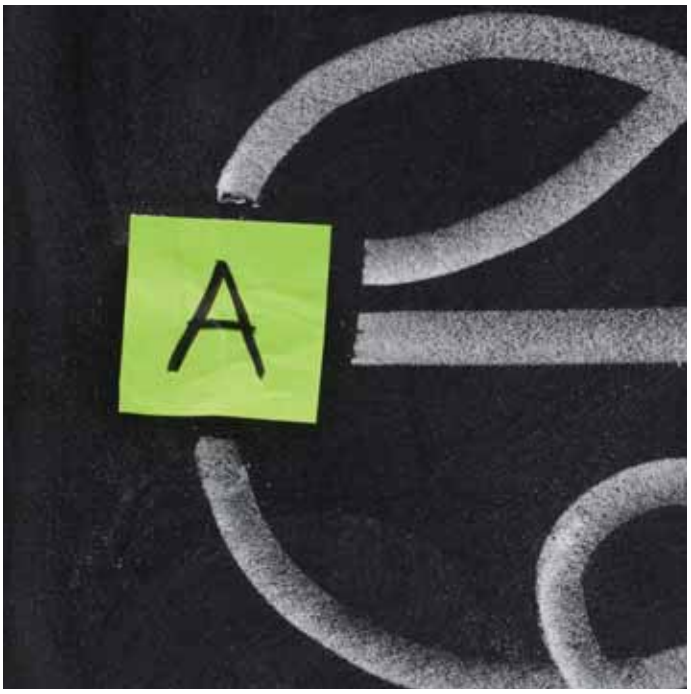
A Yes, finding the leak in your plumbing means following along the pipes to the source (and maybe tearing open a wall). More fundamentally, fixing a business process starts with understanding it. Focusing on fixing (not just reporting and counting) drives value. The good news is that there are many techniques to make this faster, easier, and more meaningful.

Q I understand the need to know the business, but this requires lots of documentation. We've tried this and got buried in paper. What tools can help?

A There are a range of business process modeling, diagramming, process simulation, and content management tools, and many financial institutions already own them. That said, success doesn't require boiling the ocean all at once. In other industries, process improvements started decades before process modeling tools were available. Even today, enterprises use manual or near-manual systems with color-coded flags, cards, trays, boxes, or wrenches/spanners to provide big benefits. One could say, "We won't do any conventional loss event modeling until the business is really understood." It's extreme, but it would focus on the "fix" over the "number."

Q Won't peers accuse me of churning the business unnecessarily when I request this information?

A First, it's your responsibility to make the request efficiently, and that includes cooperating with other areas of your institution seeking similar information. You also can team with other units to get the analysis done more quickly. Second, if the business lines, product managers, operations managers, and others don't already have this line of sight in their end-to-end business processes (including dependencies on automation and integration), then you are flagging a major operational risk to the business. It's not churn to expect a business manager to know his or her area. *Continued on page 82*



MARKWILLIAS/SHUTTERSTOCK

These are not just the "big bads" like huge frauds or hurricanes. They also include the range of daily operational costs and delayed or lost revenue from problems in operational processes. These add up to big numbers. Capturing them enables you to present the full benefits in business cases for improvements. For example, the same action that could avoid litigation losses arising from a know-your-customer situation also could help you cross-sell more effectively to customers.

Deliverables: A series of robust scenarios, including magnitude and frequency in view of prior cascading or coincidental root-cause events.

3. *Understand the implications for the business.*

- At this point, we bring together 1) a dependency and root-cause view of how processes work, and 2) robust scenarios of how those processes can fail because of external or internal causes—whether space shuttles, trading systems, your car, or mortgage lending. By bringing these together, you can engage your business leaders in a discussion of how the various root causes (again, including cascading or conditional and coincidental events) can hurt their personal business metrics (such as revenue, cost, and customer satisfaction). This discussion should include all the losses they can suffer, not just basic compliance categories. Here, it is helpful to draw from the lessons of other industries that face rare events, such as plane crashes, major electrical outages, or drowning deaths at waterfronts.

Grounding the analysis in root-cause occurrences yields a far more concrete result than estimation based only on

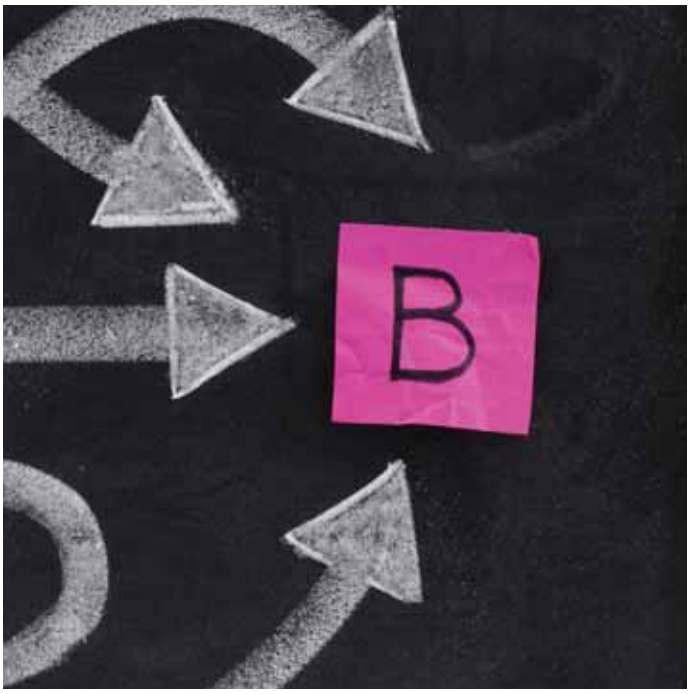


Table 1

Key Changes in the Shift to a More Direct Approach to Ops Risk

Activity Area	From…	…To
Focus on operational risk outcome	Compliance	Business value, risk-adjusted return on capital
Depth of business-line understanding	RCSAs	How the business works and real threats to real operations globally
Numbers of events available to analyze	x	100x or more
Reporting approach	Summaries	Insights into patterns of potential problems, with a focus on levers for improvement
Operational risk handoff to the business	Reports	Joint action plans for improvement and capital budgeting
Financial perception of operational risk management	Overhead	Insight into cost reduction and product opportunities
Ease of closing business case for improvement projects	Difficulty in establishing direct linkage from process improvements to capital calculation	Clearer line of sight with more data points and more direct cause-and-effect chain
Business-line leader reaction to ops risk management	Cringing at an ugly allocation	Gaining insights into growing revenue through flexibility, less cost, and reduced operations risk

sparse data from rarer loss events. It's a two-way process. Root-cause-grounded models make it easier to predict resulting loss events, especially less frequent ones. The prediction quality is driven both by number of data points and by breaking down the process into pieces and applying realistic views of what could go wrong.

Some risk disciplines refer to this as "structured judgment" because it reduces the rough guesses, breaking it into more tangible pieces that are easier to estimate. This is the same process used by, for example, CFOs and sales leaders to obtain more realistic quarterly sales estimates. With this approach, root-cause events become visible levers for improvement to metrics that business-line managers care about: reducing cost, increasing revenue, and improving customer satisfaction.

- The ability to detect root causes is reflected at this point. A factor is included in the model (as simple as a "0" or "1" in a spreadsheet) to indicate threats and adverse events that the institution lacks a good way to detect. Events detected too late are more likely to be worse. If a sports team doesn't know that a player is out sick until game time, that's a detection problem for the team. Detecting "unknown unknowns" or "dark corners" is crucial. Improved ability to detect root causes turns on the light and makes those dark corners go away. Many unknown unknowns are well known to someone who has "been there and seen that." For example, could a team come back from three games down to win a pennant in major league baseball?[6]
- Good detection also avoids asymmetric information problems. In the typical office sports pool, participants eagerly search out key information to reduce their risk. Yet, in trading, many managers (line and risk) have difficulty seeing or calculating the true risk of products in which traders have positions. Thus, they set incorrect limits. Traders seeking profit then exploit these limit errors. The rest is history.
- Once this picture of the business is painted, it becomes easier to identify 1) priorities for improvement, and 2) solid business cases for improvement. The business-case data is generated by comparing the cost of the improvement to the benefits received (at the stage of the fix and downstream improvements). Benefits include lowering costs, enabling revenue, improving customer satisfaction, and reducing capital.

  Deliverables: A risk-aware business improvement model, including the detection factor and the allocation to business lines and functional owners.

The next step is to fix the risk-causing problems to

Continued from page 80

Q Won't we still have debates about the frequency of resulting loss events?

A Looking at consequent loss events in terms of root-cause events will at least be far more testable and will offer a proposed fix or lever for improvement—a business rule and its implementation in an IT system. This approach is part of the more "structured judgment" (discussed in the article).

improve business performance. These specific improvements can then be used to both refine the operational risk capital model and justify reductions based on the specific improvements. But those are subjects for future articles. For now, the operational risk manager has created a data-driven seat at the table to help guide business owners to better performance results.

Conclusion

While the industrial approach described here offers business benefits in terms of performance outcomes, simplified governance, and organizational engagement, its greatest benefit may be this: to break the negative cycle that often surrounds operational risk. Because this approach provides simpler and clearer levers for fixing operational problems and delivering several types of value to the business, the operational risk manager has the opportunity to play a new, positive role—that of change agent. This is your personal opportunity today. ❖

Gabriel David *is a specialist in enterprise risk management and restructuring. He has worked with many global financial institutions and G-20 regulators. Contact him at* gabedavid@gmail.com. ***Brian Barnier*** *is a principal at ValueBridge Advisors. He has worked in operations, risk/quality management, and regulatory issues in several industries; serves on industry best-practice committees; teaches professional education; and researches and advises on improving effectiveness. He contributed to the book* Risk Management in Finance, *published by Wiley & Sons. Contact him at* brian@valuebridgeadvisors.com.

Notes

1. Bank for International Settlements. 2009. *Results from the 2008 Loss Data Collection Exercise for Operational Risk*. Basel: BIS Press and Communications.

2. Barnier, Brian. 2009-10. "Ten Questions in Operational Risk Today and Insight from Other Industries." *The RMA Journal* (December-January).

3. Sidler, Christoph, and David, Gabriel. 2003. "Impact of the New Basel Accord." EDS Publishing.

4. Detailed guidance to address the dependencies of operational processes on IT is provided in ISACA's *Risk IT: Based on COBIT* (www.isaca.org/riskit). This is especially helpful because it contains both a framework and implementation guidance. ISACA guidance already is cited on the U.S. FFIEC website, although this does not imply a regulator endorsement in a specific situation or a safe haven in using it.

5. Effective scenarios are more than pieces of processes or single events. Financial institutions are part of complex systems, and thus a systems approach is more appropriate. For additional guidance on scenarios, see the scenario analysis section of the ISACA *Risk IT Practitioner Guide* (available at the www.isaca.org bookstore). Also useful is scenario analysis guidance from industries and disciplines such as oil and gas, electric utilities, airlines, hospitals, emergency medical services, business continuity, or corporate finance (especially around supplier prices and foreign exchange rates).

6. Yes, they can. See http://www.boston.com/sports/baseball/redsox/articles/2004/10/21/story_is_too_good_for_words