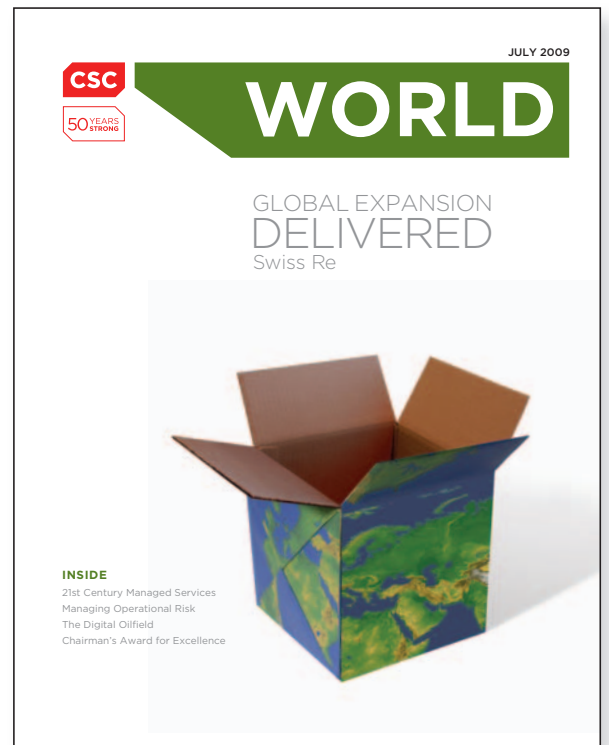


CSC

AN ARTICLE FROM

CSC
WORLD

FIRST HAND:
Managing Operational Risk,
an Interview With Bob Flast



JULY 2009

MANAGING OPERATIONAL RISK

AN INTERVIEW WITH BOB FLAST

Enron collapses. The Exxon Valdez spills 270,000 barrels of oil. Barings Bank is brought down by a rogue trader. Mattel recalls 19 million toys. What do these events have in common? They all represent losses due to failures of people, processes or systems. And there are no excuses for any of them, according to Bob Flast and Dennis Dickstein, authors of *No Excuses: A Business Process Approach to Managing Operational Risk* (Wiley, December 2008).

Flast, a CSC management consulting partner, and Dickstein, a risk manager in financial services, often shared work stories as neighbors and friends. One day, Dickstein was recounting operational risk management (ORM) activities aimed at identifying and mitigating potential failures in processes, systems and people. Flast, an expert in business process management (BPM), noted that if a company used a BPM approach to design, develop, deploy and monitor its processes in the first place, many of those risks could be mitigated or avoided completely.

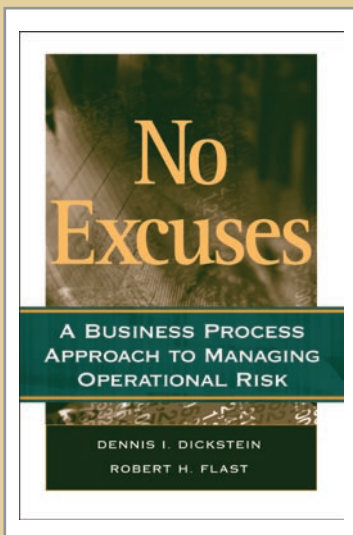
They joined forces to write *No Excuses*, which offers readers a step-by-step guide for aligning and integrating ORM into your organization's business flow. We spoke with Flast about the relationship between BPM and operational risk, and how the book can help organizations develop long-term solutions for managing risk.

What is operational risk, and how does it compare with other types of risk?

Flast: There are risks you choose to incur as part of doing business, such as credit or market risks. These are expected. And then there are risks you do not choose to incur, such as risks to your reputation or bottom line. Operational risks fall into this category. Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Employees can intentionally or unintentionally make mistakes or fail to follow existing policies and processes. Deficiencies in an existing procedure, or the absence of a procedure, can result in losses. Automated processes and systems, plus the underlying technology, security or infrastructure, can break down and cause losses. In most operational risks, process is the common denominator.

Your book cites many industry examples of operational risk and its effects, like the Exxon Valdez oil spill and commercial airliner crashes. What do they have in common with a single rogue trader bringing down Barings Bank?

Flast: In each of those unfortunate events, investigators ultimately found that there was a problem with people, processes or systems. In the cases of the Exxon Valdez oil spill and Comair crash, there was a "people" failure, as well as possibly process failures. It's easy to dismiss Barings Bank's catastrophe as a renegade trader committing fraud. But if the processes and organizational controls had been properly designed and enforced, a rogue trading incident would have been more quickly detected, if not prevented altogether.



Author Bob Flast

How would a BPM approach to ORM have helped in these and similar cases?

Flast: As I mentioned earlier, process is a common denominator in the three sources of operational risk. Therefore, it makes sense that a business process management approach to systematically designing, simulating, developing, deploying and monitoring processes would be a valuable tool with which to anticipate, avoid or mitigate operational risk. Take, for example, the huge power blackout in the Northeast United States in August 2003. Using a BPM approach to testing the automated and manual backup processes and to failure simulation — both, intended to avoid blackouts — would have surely lessened the likelihood of failure or, at least, minimized its duration. That is why we joined BPM and ORM in our Integrated Framework.

How difficult is it for an organization to integrate their existing business processes with operational risk management?

Flast: I don't think it would be a particularly challenging integration for most organizations to pursue. Structurally, BPM and ORM are more similar than they are dissimilar. The idea of monitoring, for example, is a critical component in both business process and operational risk management life cycle frameworks. Other elements in the BPM framework are also neatly and clearly aligned with the major steps or activities in the ORM framework.

What is the role of IT in ORM?

Flast: Clearly, one category of operational risk is the risk of loss due to failure of systems. For example, the loss of customers and market share when your IT allows hackers to steal your customers' credit card

“THE TONE HAS TO COME FROM THE TOP. TAKE ENRON, FOR EXAMPLE. IN SPITE OF A 60-PAGE CODE OF ETHICS, PEOPLE AT THE TOP OF THE ORGANIZATION WERE FLAGRANTLY ABUSING THE COMPANY’S ETHICS.”

numbers. However, while technology is a source of risk, it's also one of the key tools that you can use to help mitigate or lessen risk, especially in designing, supporting and enabling your business processes.

The ways that you can do that are varied. Certainly one has to do with the way you develop and test systems themselves to avoid their failure. But systems can be used to catalog and manage risks. Risk databases can be consulted to provide inspiration as you think about the potential risks that confront your enterprise or your business. If the database doesn't exist already, then — as you experience risks — you can use one of the many risk management tools available.

Tell us about the chief risk officer (CRO) role.

Flast: The CRO is one of the new organizational roles that have emerged in response to operational risk, as well as to credit and market risk. In our book we talk about the typical roles, responsibilities and accountabilities that we envision for the CRO. These include setting risk management policies and procedures, and communicating results.

Is the CRO responsible for managing culture change, which must be an essential part of risk management?

Flast: I think the CEO and the board have the responsibility to do that, and the CRO is an agent of theirs in that respect. The CRO could be the spokesperson or the

champion, but the tone has to come from the top. Take Enron, for example. In spite of a 60-page code of ethics, people at the top of the organization were flagrantly abusing the company's ethics. The tone not only has to be set by the leadership, it has to be followed, as we see in the book's Johnson & Johnson case study. Their credo emphasizes their responsibility to everyone who uses their products and services, and it was essentially the basis for their very immediate and responsible reaction to the Tylenol contamination in 1982. Aligning your organization's appetite for risk with your business goals by clearly acting in accordance with your risk principles — that is the first step in ensuring you are setting the right tone.

You compare the CRO to a fire marshal, as opposed to a firefighter. Explain that analogy.

Flast: The distinction that we make between the fire marshal and the firefighter is largely one of being reactive versus proactive. A lot of our current-day approaches to risk management are like putting out fires. We wait for some event to happen and react to it. Then we decide whether it's a one-time event or represents a systemic problem that's going to recur. If it might recur, we consider whether and how to prevent it from happening again or how to lessen its impact. That's what a firefighter does.

A fire marshal is somebody who's much more preventative and proactive. As you introduce plans for a new structure or new building, or introduce new floor plans, the fire marshal considers the potential for risk, as opposed to waiting for something to happen. The fire marshal operates at a higher level, trying to forecast and asking the important questions about consequences. Every organization needs a “risk” fire marshal in addition to their firefighters. ●

“IT’S EASY TO DISMISS BARINGS BANK’S CATASTROPHE AS A RENEGADE TRADER COMMITTING FRAUD. BUT IF THE PROCESSES HAD BEEN PROPERLY DESIGNED AND ENFORCED, A ROGUE TRADING INCIDENT WOULD HAVE BEEN MORE QUICKLY DETECTED, IF NOT PREVENTED ALTOGETHER.”



BUSINESS SOLUTIONS
TECHNOLOGY
OUTSOURCING

Worldwide CSC Headquarters

The Americas

3170 Fairview Park Drive
Falls Church, Virginia 22042
United States
+1.703.876.1000

Europe, Middle East, Africa

Royal Pavilion
Wellesley Road
Aldershot, Hampshire GU11 1PZ
United Kingdom
+44(0)1252.534000

Australia

26 Talavera Road
Macquarie Park, NSW 2113
Australia
+61(0)29034.3000

Asia

139 Cecil Street
#06-00 Cecil House
Singapore 069539
Republic of Singapore
+65.6221.9095

About CSC

The mission of CSC is to be a global leader in providing technology enabled business solutions and services.

With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients, and improve operations.

CSC makes a special point of understanding its clients and provides experts with real-world experience to work with them. CSC is vendor-independent, delivering solutions that best meet each client's unique requirements.

For more than 50 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.

The company trades on the New York Stock Exchange under the symbol "CSC."

CONTACT CSC WORLD: world@csc.com

VISIT: www.csc.com/cscworld