CONNECTICUT
BANKING
The official magazine of the Connecticut Bankers Association
First Quarter 2009

Enterprise Risk Management

A SUPPLEMENT TO
The Commercial Record

Enterprise Risk Management

David B. Sidon CPA

The Navis Group

Enterprise Risk Management a/k/a/ERM. What is it? It might take a War and Peace length book to explain and cover all the intricacies and interpretations, but if you'll invest 2 or 3 pages worth of your reading time, I'll do my best.

If you're a bank officer or director you are hearing or reading about ERM in innumerable disparate ways as you desperately attempt to understand ERM as a concept, as a best practice, as a strategy, as a compliance requirement.

There are two "levels" at which ERM is generally discussed. At a higher level, enterprise risk management encompasses broad-based entity-wide strategies. For banks, such would include merger and acquisition decisions, C-level employment decisions, branching strategies, and of late, the "to TARP or not to TARP" debate. On a more granular plane, ERM considers financial and operational risks at the process level. For banks, ERM might conjure up thoughts of FDICIA or SOX controls analysis regarding wire transfer authority or technology security or other process integrity issues.

Sarbanes Oxley legislation and compliance has spawned the seminal document addressing ERM. In September, 2004, COSO (the Committee of Sponsoring Organizations) (how's that for a meaningful descriptive name?) issued "*Enterprise Risk Management – Integrated Framework*", offering this definition of ERM:

> *"Enterprise risk management is a process, effected by the entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that might affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."*

Before I address the merits of whether this definition provides any clarification, I would be remiss not to recognize our college English professor who would now be going off about run-on sentences, asking whether we are talking about effecting, applying, designing, managing or achieving just what exactly? "I remain unenlightened, son."

The COSO guidance does offer a better look at ERM once you get past the cumbersome formal attempt at definition. Sometimes a list suffices, as COSO suggests that "*ERM encompasses*:

- *Aligning risk appetite and strategy*
- *Enhancing risk response decisions*
- *Reducing operational surprises and losses*
- *Identifying and managing multiple and cross-enterprise risks*
- *Seizing opportunities*
- *Improving deployment of capital"*

My personal favorite in this list is the reducing surprises part. Do Lehman, WAMU, Fannie/Freddie come to mind? All flippancy aside, I would encourage you to consider the positive and proactive language in this list. As we all initially and naively consider ERM as a cost, no-benefit exercise, "enhancing", "reducing", "seizing" and "improving" are all words that should inspire a second look.

Over the past few years I've worked at the "ERM-thing" with bankers as well as students at CT Banking Association's School of Financial Management. Recently, I've had the opportunity to bring "ERM 101" to a Board retreat, eliciting some rather interesting debate about risk appetite (more about that later on). The one lingering theme that surfaces is the matter of practicality, of efficiency, of making ERM work in a positive and proactive manner for the bank.

Let's try this.

Here are some famous and relatively familiar equations:

$E = mc^2$ $a^2 + b^2 = c^2$ h / ab = .avg inc / eq = ROE $\pi = c / d$

Here's a made-up equation to perhaps serve as a memory trick:

ERM = (ERM + ERM + ERM) / ERM

Where: ERM (Enterprise Risk Management)

Equals: ERM (Every Risk Measured) and ERM (Every Risk Mitigated) and ERM (Every Risk Monitored)

Divided and conquered through a process of: ERM (Efficient Risk Management)

Here's the crux of the matter. When we do IT risk assessments, GLBA risk assessments, DRP/BCP risk assessments, vendor risk assessments, operational risk assessments, asset-liability modeling, internal audit, branch security reviews, BSA risk assessments, and so on, and so on, we are risk managing. But oh, the inefficiencies and disconnects, don't you agree? And seemingly, each of those risk components represent cost centers in your mind's eye.

Efficiency #1:

If we continue to do each of these risk analyses in silos (see Efficiency #2 – "why do we do these risk analyses in silos?"), how do we make the leap that might provide payback for our efforts? IT risk assessments are a great example. Regulatory compliance demands a process that we take a look inward and assess each piece of our technology realm; hardware, software, and critical technology vendors. Reams of documents (or giga-bytes of storage for those of you that have really gone green) have been created. To what end? To appease the regulators? Well, yes, mostly. How did your bank benefit from the exercise? Likely not at all, unless you diligently asked, like a two-year old, "why?", "why?", "why?" And when something was identified as high risk, did you ask the "so now what?" question, or were you merely satisfied that "yep, by golly, we identified all them-there what ya call high risk rated things"? Not looking to insult here, but rather looking to exaggerate for impact. You <u>want</u> to find improvements!

Recently one of my client banks undertook a really diligent approach to IT risk efforts. I can't take much credit for the effort, I only kicked them off with a methodology and then they were off and running. They amazed themselves and found some persnickety control improvements that had escaped the eyes of internal auditors and intrusion testers alike. They were small things, but isn't it always the small things ….

Efficiency #2:

You remember. The "silo" question.

Do you identify some critical processes in your business continuity plans? And then identify certain critical processes where GLBA issues might come into play? And then identify certain processes for internal audit's operational control assessments? And then identify certain processes at year end for the external audit firm's operational control risk assessment (probably in a format they gave you)? You see where this is headed. Inefficiency. One thorough process map aligning process names, definitions, and owners that serves as a single "table of contents" is a great place to start. Taking this logic another step further, it is easy to imagine combining all risk assessments relative to operating processes into a single effort. While we analyze a given process for IT risk, doesn't it seem logical to consider all risks while we're around the table?

Efficiency #3:

Demand process improvement. Ask the question. Is this best practice? Is this a rule? Or is this tradition? SOX compliance stresses the concept of "tone from the top". Both high-level ERM or process level ERM benefits from an unequivocal expectation set forth by top management to honestly consider process improvements and efficiencies.

Defining risk tolerance

Consider that there are only four answers available: high, moderate, low, or not applicable. Risk, like beauty, is in the eye of the beholder. So what's the criteria? Your own judgment? Regulatory guidance? Guidance from senior management? Or a strict definition of risk tolerance as approved by your board of directors?

Here's a recommendation. This question is a great agenda item for board strategic planning. If the board defines risk tolerance once and for all, in an unambiguous manner, all managerial risk assessments have a solid and consistent foundation.

Here's an approach. First, if there is no risk for a given banking process, so state. It's OK. Really! "N/A" is indeed an acceptable outcome of your risk analysis; in fact, determination of risk-or-not is an important starting point. Then, rather than getting stuck in the "significant-some-minimal" conundrum, look to a financial measure as a guide. Even reputation and compliance risks may be reduced to cost analysis/judgment.

The regulatory view

The banking industry has "experienced" enterprise risk management as a discipline since FDICIA was enacted in 1991. I think we would all agree that much has changed in our industry in the last 18 years, let alone the last 18 months. However, in many institutions the methodology used to comply with FDICIA requirements has changed little in that time frame, with seemingly little pressure from either regulators or auditors to upgrade the methodology. Thanks to the Sarbanes Oxley legislation, COSO offers a more enlightened approach to risk analysis and relevant audit standards have caught up to a new risk-based methodology. Our regulators as usual are reluctant to demand a particular approach; we all remain free to choose poorly and then be audit-corrected to the best practice.

So what's the requirement with respect to our approach to enterprise risk management? My research (thanks to some assistance from the FDIC) turns up a very important "hint". In the FDIC's "Risk Management Manual of Examination Policies, Section 4.2 – Internal Routine and Controls" the following paragraph seems to sum up this entire discussion.

> *"Internal control is a process designed to provide reasonable assurance that the institution will achieve the following internal control objectives: efficient and effective operations, including safeguarding of assets; reliable financial reporting; and, compliance with applicable laws and regulations. Internal control consists of five components that are a part of the management process: control environment, risk assessment, control activities, information and communication, and monitoring activities. The effective functioning of these components, which is brought about by an institution's board of directors, management, and other personnel, is essential to achieving the internal control objectives. This description of internal control is consistent with the Committee of Sponsoring Organizations of the Treadway Commission (COSO) report entitled Internal Control-Integrated Framework. Institutions are encouraged to evaluate their internal control against the COSO internal control framework if they are not already doing so."*

For emphasis, re-read that last sentence. COSO is indeed the methodology encouraged, thereby begging the question of the viability of our 18 year-old (and tired) FDICIA matrices.

The move to enterprise risk management as a way of life for our industry has placed some stresses on our organizational structures and budgets. As the internal audit function is seen more and more as merely an assessment tool, and given less credence as an actual "control", outsourcing of the internal audit function is growing. The subject-matter expertise needed for the myriad of compliance and control issues facing today's industry is difficult to foster in a small team sequestered within the walls of one institution. The industry is migrating away from the senior internal auditor to a more pro-active chief risk officer role.

The "shift" is easier than one might imagine. The senior internal auditor and his/her department have traditionally reported to the Audit Committee of the Bank's Board. This is a time-tested, industry acknowledged best practice and appropriate segregation of accountability. The shift? The Chief Risk Officer and his/her department report to the Audit and Risk Committee of the Bank's Board. The focus

of a risk department will be different than the focus of the traditional internal audit group. The re-focused Board committee will need to shift to a risk-based mindset. Important to this shift is a fresh look at the committee's charter.

The message that I would like to leave is that enterprise risk management should be a discipline embraced throughout the organization, with a managerial "dictate" that ERM be used to benefit the institution, to introduce risk-based wisdom into the mix. The financial industry has been taken by surprise too many times in the last few years. Although there is no single silver bullet to forever remove the element of surprise, a thoughtful approach to risk should help. That's enterprise risk management.

David B Sidon, CPA (sidon@navis-group.com) is principal of The Navis Group, a risk management consulting firm based in Gloucester, Mass., specializing in enterprise risk management and business continuity planning – www.navis-group.com.