Top 10 answers from the world's first Chief Risk Officer

Read what James Lam, President of James Lam and Associates, Enterprise Risk Management Specialists, says in response to the top 10 questions received during his recent Web seminar with Cognos, an IBM company. As an Author, Consultant, and former Chief Risk Officer, Lam speaks with an authority that few others can match in the emerging risk management discussion.

Q: Define what you mean by Enterprise Risk Management (ERM) and its component parts?

A: In my first book *Enterprise Risk Management – From Incentives to Controls*, I defined ERM as:

"An integrated framework for managing credit risk, market risk, operational risk, economic capital, and risk transfer in order to maximize firm value."

While strategic and business risks were implicit in my definition for operational risk, I now believe they deserve explicit treatment. In my current work, and also in my upcoming second book, the definition of ERM has been expanded to explicitly include business risk and strategic risk. This evolution reflects my own education and experience, as well as industry practices. I believe business and strategic risks are the most critical risks for business enterprises, and as boards and executive management become more involved in ERM, their inclusion will be a natural outcome in the future.

Therefore, within the context of ERM my definitions of the five major categories of risk are:

- Credit risk. Risk/return trade-offs due to loan or counterparty credit default
- Market risk. Risk/return trade-offs due to market price movements (e.g., interest rate, FX, equity, commodity)
- Operational risk. Risk/return trade-offs due to people, processes, systems, or external events
- Business risk. Risk/return trade-offs due to revenue volatility, where revenue flow may be insufficient to cover fixed expenses (current business)
- Strategic risk. Risk/return trade-offs due to strategic decisions on organic growth and acquisitions (future oriented).

Q: Is there a tool or software application out there that provides for metric measurements of risk enterprise-wide? How many companies are actually implementing dashboards? How important is this?

A: There are some software products that include dashboard reporting as part of their functionality (vendor specific). However, I think the most valuable dashboard applications would integrate information from disparate systems and databases (vendor neutral). [Author's note: for an example, please see www.cognos.com/dashboards.]

I think developing an ERM dashboard is one of the hallmarks of success in ERM. The purpose of an ERM dashboard is to aggregate risk information, develop an enterprise-wide view of risks, and disseminate role-based risk information to the appropriate people. Recently I spoke at the 2007 ERM Symposium and asked how many companies were implementing dashboards, and more than 50 percent of the over 100 attendees raised their hands.

COGNOS®
AN IBM® COMPANY

Q: Who are the right people to start an ERM practice, what is a better title for Risk Managers, and do you need a Chief Risk Officer for effective ERM or can these responsibilities be distributed across functional managers?

A: It depends on the organization and level of maturity of its ERM program, as well as the competencies of the staff. It is essential that the ERM group is supported by executive management and the board. Companies operating in risk-intensive industries with over $1 billion in annual revenue are increasingly appointing CROs, but the CFO is someone who also needs to support an ERM program. Regardless, the responsibilities for many aspects of ERM (e.g., business and operational risks) should be distributed to business and functional groups.

Q: How do you approach an ERM implementation if there are already various existing systems in place?

A: Nearly all companies have some existing risk management policies, systems, and processes in place. In terms of ERM implementation, I think it is critical to understand the board's and management's expectations for ERM, establish and clearly state the vision or goal for the overall ERM program, and develop a clear multi-year plan with well-defined milestones and measures of success. A successful ERM implementation is about more than just meeting compliance requirements or developing an ERM framework; it is about integrating risk management thinking and tools into business processes in order to optimize business performance.

Q: What do best practice ERM programs entail?

A: The hallmarks of success in ERM that I look for include the following:

- An engaged senior management team and Board of Directors
- Established policies, systems, and processes, supported by a strong risk culture
- Clearly defined risk appetite with respect to risk limits and business boundaries
- Robust risk analytics for intra- and inter-risk measurement, summarized in an "ERM dashboard"
- Risk-return management via integration of ERM into strategic planning, business processes, performance measurement, and incentive compensation.

Q: How frequently should risk assessments be done?

A: At most companies risk assessments are performed annually. Leading companies are also updating their risk assessments on a monthly or quarterly basis. More importantly, risk assessments should be performed using a top-down risk-based approach so the most critical risks can be identified and the risk assessment processes can be rationalized. In other words, a more detailed process—including documentation, process mapping, measurement, and reporting—should be applied to the most critical risks, while a streamlined process should be applied to the other risks.

Q: Can you elaborate on the integration of ERM into strategic planning processes? Is this mainly a reporting issue?

A: I believe the integration of ERM into strategic planning (often referred to as strategic risk management) is the next frontier in risk management. It is more of a management issue, but reporting is an important component. When I helped start a capital markets business at GE Capital, we had a corporate process called Policy 6.0. We had to clearly define the key business and financial assumptions underlying our business plan. More importantly, we established key performance indicators, key risk indicators, and "trigger points" for management decisions and actions. On a quarterly basis, we conducted business/risk reviews with corporate management and made key changes to our business and risk strategies based on market opportunities as well as our business performance.

Q: **In addition to the process and system implementation, do you have any items that should be specifically stated within an ERM policy?**

A: An ERM policy should include a common risk taxonomy, risk tolerance levels for key risks, and risk assessment, measurement, and reporting requirements. Some ERM policies also include specific risk escalation levels, such as loss or business impact thresholds, to ensure emerging risk issues are escalated and addressed in a timely manner.

Q: **As a Chief Security Officer, how can I tie my enterprise security risk assessments into an ERM program?**

A: As a former CRO, I think the CSO has three important roles to play in ERM. The first is to ensure that corporate-wide policies and standards are established for information security (including end-user computing, privacy, and more) and that business units are in compliance with these policies and standards. Second, I looked to the CSO to help improve the quality of risk assessments, key risk indicators, and reporting related to information security. Finally, since the CRO office deals with highly sensitive information, I solicited the expert input from the CSO to ensure that effective information security controls were in place for the risk management systems, databases, and dashboard reporting.

Q: **How do I help the CIO integrate a strategic technology plan with ERM?**

A: First, you can help the CIO to leverage ERM to identify the strategic, business, and operational risks associated with the strategic technology plan (including outsourcing risk, technology risk, and other key factors). The technology plan should also support the ERM program in terms of the risk management systems, database, and reporting initiatives. I have worked on over 50 ERM engagements, two as CRO and the rest as a Consultant, and I can tell you that IT has been a critical component in each one of those engagements.

For more information on these and other related topics, please visit these addresses:

White Paper: *Emerging Best Practices in Developing Key Risk Indicators and ERM Reporting* by James Lam and Associates
http://www.cognos.com/pdfs/whitepapers/wp_best_practices_deploying_key_risk_indicators.pdf

Risk Management Reporting Demo
http://www.cognos.com/solutions/demos/risk_management/index.html

More Risk Management Resources
www.cognos.com/banking

Contact an ERM representative

To contact a Cognos Enterprise Risk Management Representative in the U.S. or Canada, please call 1-800-426-4667 and choose option 4. Contact numbers for other areas can be found at www.cognos.com/contact.

About James Lam and James Lam & Associates

Founded in January 2002, James Lam & Associates (JLA) is a consulting firm singularly focused on risk management. In a 2007 Euromoney survey, Mr. Lam was nominated by clients and peers as one of the leading risk consultants in the world. Mr. Lam has over twenty years of experience in risk and business management. He is widely noted as the first ever "chief risk officer" and an early advocate of enterprise risk management. Previously, Mr. Lam served as Partner of Oliver Wyman, Founder and President of ERisk, Chief Risk Officer of Fidelity Investments, and Chief Risk Officer of FGIC Capital Markets Services, Inc. Mr. Lam is the author of *Enterprise Risk Management: From Incentives to Controls*, which has ranked #1 best selling among 25,000 risk management titles on Amazon.com. For two years in a row (2005 and 2006), *Treasury & Risk Management* magazine named him one of the "100 Most Influential People in Finance." More information on JLA can be found at **www.jameslam.com**.

About Cognos, an IBM company

Cognos, an IBM company, is the world leader in business intelligence and performance management solutions. It provides world-class enterprise planning and BI software and services to help companies plan, understand and manage financial and operational performance. Cognos was acquired by IBM in February 2008. For more information, visit **http://www.cognos.com**.

For more information

Visit the Cognos Web site at www.cognos.com

Request a call

To request a call or ask a question, go to www.cognos.com/contactme A Cognos representative will respond to your enquiry within two business days.

(02/08)

COGNOS®
AN IBM® COMPANY