


Risk Management Goes Real Time

Gartner SYMPOSIUM ITXPO 2002



U.S. Symposium/ITxpo
6–11 October 2002
Walt Disney World
Orlando, Florida

Douglas McKibben

Risk Management Goes Real Time

Douglas McKibben, 52J, SYM12, 6-11 October 2002



No surprises, please—we're in risk management.

Investors and regulators are demanding leadership, accountability and decisive, transparent action from executive management. At the same time, the market has demonstrated a low level of tolerance for surprises that adversely affect earnings, whether it's an accounting snafu or an operational loss. Both have a negative effect on the reputation of the organization and on shareholder value.

As a result, concerns about operational risk have emerged from the back-office and are no longer the sole domain of internal auditors. Operational risk is a frequent topic of speeches by the Federal Reserve and other regulatory bodies. And for the banks that paid little attention before, the Bank for International Settlements' New Basel Capital Accord, which proposes a separate capital charge for operational risk, got their attention.

So, how do you deal with the issue?

Risk Management Goes Real Time

Douglas McKibben, 52J, SYM12, 6-11 October 2002

Gartner | G2

Viewpoint

- Organizations must measure operational risk to effectively manage risk exposures.
 - Determine frequency and severity.
 - Evaluate risk-control processes.
 - Allocate capital.
- Limited data, complex interdependencies and the lack of an integrated approach to risk inhibit the measurement of operational risk.
 - Difficult to identify and quantify operational risk.
 - Requires cross-industry data.



© 2002 GartnerG2


Viewpoint: Operational risk is not easily identified.

Chief financial officers are expert at managing market and credit risks, and minimizing the variability of return and loss exposure for cash or other assets. Operational risk—the exposure to uncertainty arising from daily tactical business activities—also exposes the organization to potential monetary loss. But operational risk is not easily identified or quantified, depends heavily on internal processes and controls, and has traditionally been the responsibility of internal auditors. It is essential to understand those internal processes and identify risk-drivers.

Developing an enterprisewide view of operational risk is further complicated because risks are embedded in lines of business and at various operations and support functions across the organization. Despite the challenge, an enterprise approach to risk management in general, and operational risk specifically, is necessary to identify, monitor and measure risks and risk dependencies to evaluate risk-control processes and to allocate capital. Operational risk must be decomposed into its basic elements so the causes, frequency and impact of losses can be identified precisely. Only then can management take effective action.

Risk Management Goes Real Time

Douglas McKibben, 52J, SYM12, 6-11 October 2002



Master risk strategies

- Operational risk is “the risk of loss resulting from inadequate or failed internal processes, people or systems or from external events.”
- Operational risk management is influenced by regulatory initiatives but driven by business demands.
 - Real-time enterprise
 - Concerns about business continuity
- Mastering risk strategies is integral to growing revenue/earnings and increasing investor confidence.
 - Limit earnings volatility and enhance shareholder value

© 2002 GartnerG2

Dynamic: Master risk strategies before they master you.


Increased emphasis on operational risk management is influenced by regulatory initiatives, the initiative to shorten settlement cycles and more demanding compliance requirements. However, operational risk management is driven by business challenges like a real-time business environment, concern about business continuity and a world where the most valuable assets may be intellectual, not physical. Companies need to limit earnings volatility/enhance shareholder value as the capital markets grow intolerant of surprises. Risk management will also be a defining factor in the cost of raising capital.

Most companies are still organizationally, functionally and technically disaggregated, which impedes business success and makes it harder to meet the demands of regulators. As business is e-enabled, the threat increases since risk materializes faster, has a greater impact and requires real-time management to avoid adverse results and to meet customer expectations.

A standardized approach to risk management validates management processes and improves internal discipline and control. This requires measuring operational risks across the enterprise and relating risks to business processes and controls, as well as to external factors and quantifiable loss profiles.

Risk Management Goes Real Time

Douglas McKibben, 52J, SYM12, 6-11 October 2002



The path forward

- Enterprise risk management will be a leading practice for most organizations by 2010.
 - Investor and industry analyst concerns about earnings
 - Regulatory capital charges for risk
 - Management of risk silos has been unsuccessful
- Operational risk management will expand from an audit-and-control approach to proactive identification to create risk transparency.
- Insurers will become more active in the measurement of operational risk and provide a wider range of related products.

© 2002 GartnerG2

Prediction: Predictive risk management tools will be invaluable.

While the regulatory efforts of the Bank for International Settlements do not bind corporations, they can look to the New Basel Capital Accord for guidance in defining, measuring, managing and allocating capital for operational risk. Moreover, the Securities and Exchange Commission is cracking down on “earnings management,” limiting the use of restructuring charges and reserves. Enlightened organizations will begin an integrated approach to risk management.

Operational risk management must be a boardroom concern that is actively managed and reported along with market, credit and other financial risks. There will be predictive analyses of operational risk levels rather than historical assessment and resolution of audit findings. Predictive risk management tools will be used to monitor key indicators. Monitoring this information on a real-time basis and in aggregate will provide insight into emerging trends, diminish the possibility of failures gaining momentum and permit an accurate view of the risk level for the entire organization.


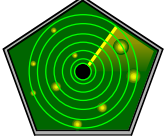

Insurers will become valued advisors in determining how risks are measured and for modeling operational risk. More insurance products will emerge based on accumulated and shared operational loss data. The price of insurance relative to the potential for reimbursement of losses will be a major consideration. Insurers will also partner with capital markets to finance operational risk.

Risk Management Goes Real Time

Douglas McKibben, 52J, SYM12, 6-11 October 2002

Gartner|G2

Dynamics

- Silo-based organizational structures impede the identification of risk dependencies. 
- Data is short-lived, not shared, and is available only at the point of failure. 
- Measurement is limited to:
 - Economic impact (balance sheet, income statement)
 - What is easily identifiable and quantifiable within the organization—linear interpolation, value at risk
 - A focus on system failures, not process failures 

© 2002 GartnerG2

Dynamic: Risk management requires an integrated approach.

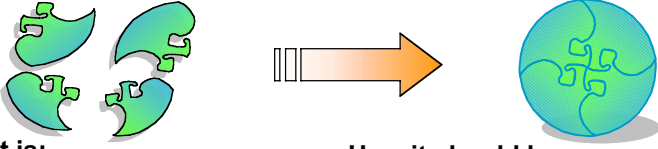
Most organizations are far from an integrated approach to risk management. Cultural limitations and business unit boundaries impede the identification of and collection of risk data. Workflow connectivity and sharing of information are often impeded by legacy systems with application-centric data that are frequently stand-alone or proprietary. Consequently, it is not possible to collect common data, identify risk interdependencies or identify exposure trends. While most banks monitor loss events, many do not actually collate the information into a loss database. Data are not captured on a continuous or consistent basis, and events are not linked across the organization. Most operational risk management has been limited to activities that can be observed and quantified. The emphasis has been on system failures, not process failures. In order to measure and manage operational risk, it is necessary to understand the complete workflow and how deficiencies in those processes may lead to operational losses. This dovetails with corporate efforts to achieve straight-through processing, which require the same analysis for a different purpose.

Risk Management Goes Real Time

Douglas McKibben, 52J, SYM12, 6-11 October 2002

Gartner | **G2**

An enterprise view of operational risk



How it is:

- Lack of standard definitions and reporting formats
- Risk data diffused across organization, embedded in various applications
- Stand-alone and proprietary systems
- Only manage what can observe and quantify
- Responsibility of internal audit

How it should be:

- XML risk data definitions and reporting formats
- Workflow connectivity and sharing of information
- Common risk management processes
- Real-time predictive analysis and reporting
- Business units maintain primary control

© 2002 GartnerG2

Dynamic: Breaking down silos serves multiple needs.

The need to eliminate fragmented and tactical approaches to system and business process integration and sharing information is not limited to operational risk management. It is the common thread that connects several other initiatives including Internet-enabled service delivery, integration of the physical and financial supply chains, and straight-through processing and faster settlement.

While historical data may be a good starting point, past risk profile and loss experience may provide little value as an indicator of future exposures (e.g., understanding the risks of establishing an e-business channel). It is also important to look beyond risks that can be readily observed or have been directly experienced. Predictive risk systems are also needed to identify potential problem areas as they develop.

While it is necessary to identify and track internal process and systems incidents and near-misses that can be measured and statistically modeled, organizations are also exposed to potential catastrophic losses from external forces and to more intangible risks such as reputation risk that may result directly from operational failure. Determining the potential frequency and severity of these latter types of events will require scenario analysis based on loss information from external sources.

Risk Management Goes Real Time

Douglas McKibben, 52J, SYM12, 6-11 October 2002



The regulatory spotlight

- The New Basel Capital Accord will introduce updated management guidelines and reserve requirements for market, credit and operational risk.
- The Bank for International Settlements is targeting 12% of risk capital for operational risk (excludes strategic and reputation risks).
- The Organization of Securities Commissions and International Association of Insurance Supervisors are also collaborating with the Basel Committee.

© 2002 GartnerG2

Dynamic: The impact of the Accord will extend beyond banking

The New Basel Capital Accord is a regulatory initiative designed to align liquidity-level requirements with actual risk. It will introduce updated management guidelines and reserve requirements for market, credit and operational risk. It also requires companies to recognize risks for related companies where they have managerial control on a groupwide basis. Senior managers of financial institutions will be accountable for the integrity of internal operational risk systems and processes. There is a legal liability, and they will be required to sign off that the institutions are in compliance with the Accord.

The Bank for International Settlements' definition provides the necessary foundation for addressing operational risk. But there is still no standard industry definition; therefore institutions are establishing their own definitions. These initiatives should follow a consistent methodology, use assumptions that are compatible with the Basel guidelines and be flexible enough to reclassify collected data should the Basel criteria change.

The Bank for International Settlements is targeting 12% of risk capital for operational risk. For purposes of calculating regulatory capital, the Accord excludes strategic and reputation risks, but institutions should not.

The Accord will probably affect institutions other than banks. The Organization of Securities Commissions and International Association of Insurance Supervisors are also collaborating with the Basel Committee.





Risk Management Goes Real Time

Douglas McKibben, 52J, SYM12, 6-11 October 2002

Gartner | **G2**

Sources of operational risk

- **Information technology:** Coding, modeling, information flow/management errors, systems and communications failures, and project overruns.
- **Operations:** System and human errors, utility failure, natural disasters, key personnel risk.
- **Workflow:** Order execution, transaction recording and clearing/settlement errors, physical delivery and documentation risks.
- **Crime:** Fraud, embezzlement, rogue trading, electronic intrusion.



© 2002 GartnerG2

Dynamic: The impact on third-party relationships

In addition to traditional back-office activities, operational risk touches virtually all business processes. These exposures extend to third-party business partners and alliances.

In general, the user of outsourcing services trades direct operational risk responsibility for business risk linked to the contract and service-level agreements. However, the user retains policy decision-making responsibility and must actively manage the relationship based on well-defined objectives. This can be particularly problematic for organizations that outsource processes overseas where the user does not have a physical presence.

Various U.S. financial regulatory agencies have published guidance for managing third-party relationships. In general, regulatory bodies subject third-party relationships to the same risk management, security, privacy and information protection policies as if the user were conducting the activities directly.

The New Basel Capital Accord will hold financial services providers responsible for their third-party relationships. Failure of third-party vendors to meet Basel operational risk standards could adversely affect the overall capital adequacy calculations for the financial institution using those services.

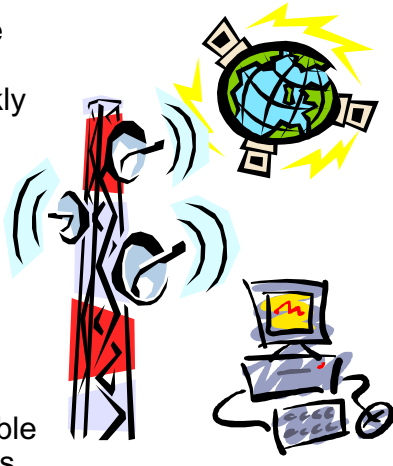
Risk Management Goes Real Time

Douglas McKibben, 52J, SYM12, 6-11 October 2002

Gartner | **G2**

Managing data

- Data model that supports the need for consistent and confidential data that is quickly accessible.
- Disciplined approach to data management.
- Clearly documented data definitions, relationships and attributes.
- Loss database that identifies historical experience applicable to current and future business activities.



© 2002 GartnerG2

Dynamic: Detailed data is key.

To manage operational risk effectively, businesses need a disciplined approach with a clearly stated and enforced plan of corporate governance. It should be a board-level concern, include standard methodology and assumptions, and ensure compliance with internal and external reporting.

The New Basel Capital Accord requires that four years of operational loss and near-miss data be collected by 2004 in order for an institution to qualify for the internal measurement approach for capital allocation. Appropriately detailed data is the key to statistical modeling, scenario analyses and planning.

One problem: Data must be recorded in sufficient detail to differentiate cause and effect, contribute to the identification of interdependencies and developing inferences from past occurrences. There is no standard way to record operational risk data to ensure sufficient detail for interpretation and audit.

In many organizations, incident data may be recorded, but it is not consistently and continuously captured, not recorded at a suitable level of granularity, not used or compared across business units and in many cases, not retained at all.

Risk Management Goes Real Time

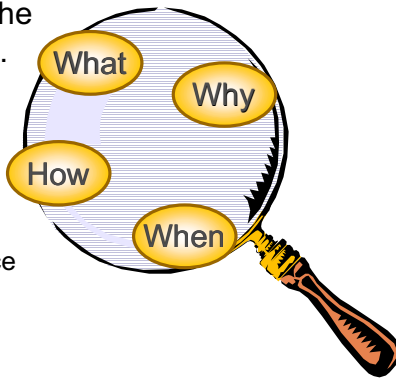
Douglas McKibben, 52J, SYM12, 6-11 October 2002

Gartner | **G2**

Data interpretation

Diversity of operational risk processes and infrastructures complicates the creation of a standard risk model.

- Interdependencies
- Impact and probability of risks
- Calibration of measurements with those of other institutions that have comparable experience



© 2002 GartnerG2

Dynamic: Multiple data analysis tools are required.

For operational risk, data interpretation is a challenge because the diversity of processes and infrastructures complicates standard modeling, and it involves complex interdependencies. Credit and market risk are generic enough to be addressed with statistical models and replicated across industries.


There are some areas of operational risk, particularly where technology is central, when a less-costly generic risk model can be applied. However, indirect exposures such as strategic or reputation risk cannot be statistically modeled. Their unpredictable nature does not permit collection of objective data, and they must be assessed based on scenario analysis.

Scenario analysis is also useful when frequency is low or must be based on experience of peer institutions. Here, internal data need to be supplemented with outside sources and benchmarked against other institutions to estimate impact and probability, taking into consideration institution size, structure and practices.

Some operational risks are correlated, such as business risks associated with political change. But overall, little research has been done regarding operational risk correlation.

Risk Management Goes Real Time

Douglas McKibben, 52J, SYM12, 6-11 October 2002



To measure or not to measure

- Approaches to operational risk capital allocation
 - **Basic indicator approach:** Single indicator as overall proxy for operational risk exposure (e.g., gross income).
 - **Standardized approach:** Indicator for each business line. Requires tracking and management assessment of loss data.
 - **Internal measurement approach:** Loss databases used to calculate probability and magnitude of expected losses by business line.
- Minimum capital can be significantly higher for institutions that do not measure

© 2002 GartnerG2

Dynamic: Three options for determining operational risk

Basel provides three approaches to determine operational risk capital.


Basic indicator approach uses a single indicator as an overall proxy for the operational risk exposure for the entire institution.

Standardized approach uses an indicator for each business line, but requires systematic collection and tracking of loss data and assessment of management. The board and senior management must demonstrate involvement in operational risk management. Indicators do not establish whether capital allocation is adequate/ necessary or provide incentive for better risk management. Capital reserves cannot be reduced unless indicators are reduced. Also, there is uncertainty as to which indicators are important.

Internal measurement approach is more likely to achieve the proper alignment of risk and capital, and a capital reduction can also produce a competitive advantage. However, once a business line approves, it cannot revert to a different standard. The cost/benefit of this more-advanced approach must be considered and also a potential floor on capital reserves that may limit the savings available to institutions short-term. In addition, justifying a case for lower capital will require an institution to reveal proprietary information about its risk management methodology and how results were achieved.

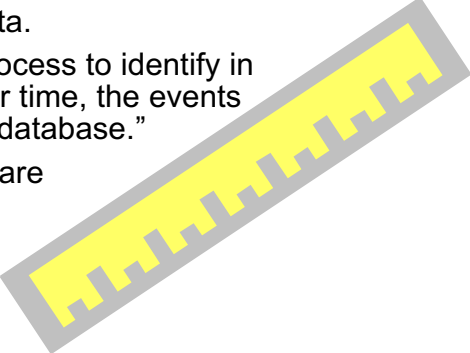
Risk Management Goes Real Time

Douglas McKibben, 52J, SYM12, 6-11 October 2002



Challenges of measurement

- Assembling sufficient data.
- Establishing a “sound process to identify in a consistent manner over time, the events used to construct a loss database.”
- Structuring data so they are clearly understood and support interpretation.
- Collecting data from internal/external sources and for both direct and indirect losses, including near-misses.
- Operating risk events are usually infrequent within an institution—compiling information can take years.



© 2002 GartnerG2

Dynamic: The obstacles to measuring operational risk

Developing measurement techniques for operational risk presents obstacles. First, it requires collecting sufficient data to estimate the probability of a loss (frequency) and the potential size of the loss (severity). It also requires an enterprisewide process to identify and record events consistently over time. This requires dividing the organization into business lines, breaking operational risk into its root causes and determining the data needed to evaluate the causes.

However, a high percentage of operating risk exposure is low-frequency and high-severity. By definition, evidence is insufficient within a single institution to substantiate a conclusive decision regarding the potential occurrence of such events. Institutions are unlikely to have experienced a statistically significant number of these events individually and will have to use assumptive scenario analyses to measure the potential for loss.

Global, industrywide data, as well as cross-industry data (e.g., manufacturing, distribution, telecommunications) for such areas as information security, business continuity and network dependability will be required to supplement and validate internal risk assessments. In addition, specialized external expertise will probably be required to assess and model such data.


Risk Management Goes Real Time

Douglas McKibben, 52J, SYM12, 6-11 October 2002

Gartner | **G2**

Risk data initiatives

- Multinational Operational Risk Exchange (MORE)
 - Sponsored by Global Association of Risk Professionals
 - Managed by NetRisk
 - Includes Risk Management Association operational risk consortium
- The Global Operational Loss Database (GOLD)
 - Managed by the British Bankers Association (BBA)
 - U.K., European, North American and Australian banks



© 2002 GartnerG2

Dynamic: Participation in the consortia isn't restricted to banks.

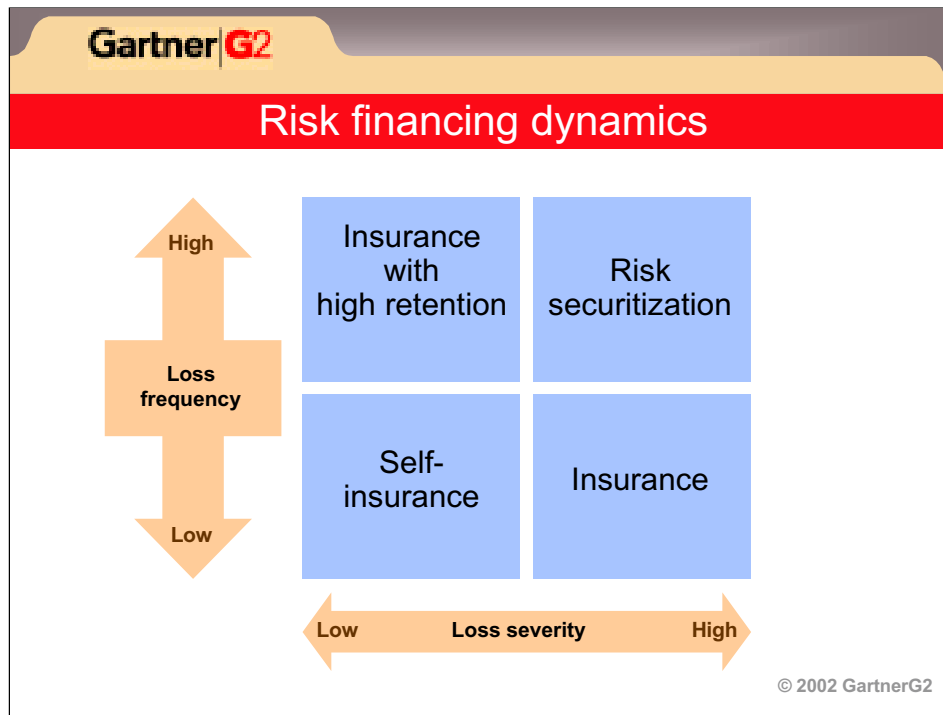
While these initiatives target financial institutions, their methodologies are applicable to any industry willing to share operational risk experience. There are several benefits to participating in such a group: a secure framework to share nonpublic loss data and retain ownership of that data, assistance in quantifying operational capital-at-risk, and access to information on predictive factors enabling managers to focus on mitigation efforts in areas with highest expected returns.

Sharing data will also assist institutions in benchmarking operational risk management practices including measurement methodologies. In addition, the data will provide actuarial estimates for creating insurance products for risk financing, which to this point have been limited due to insufficient frequency and severity information. Conventional insurance products historically focus on high-frequency, low-severity events for which there are more data.

The consortia are also actively involved in influencing the decisions of regulatory bodies regarding operational risk.

Risk Management Goes Real Time

Douglas McKibben, 52J, SYM12, 6-11 October 2002



Dynamic: Selecting the right insurance option

There are generally accepted practices for selecting the most appropriate means of mitigating risk:

Low-frequency and low-severity exposures, such as theft of office equipment, are usually financed internally through a self-insurance program. These risks have a high level of predictability, and retaining the risk is more economical than insurance.


Risks with high-frequency and low-severity, such as automobile physical damage, are usually insured, with a substantial deductible or retention, using the insurance as a catastrophe hedge.

Risks with low-frequency and high-severity, such as fire, lend themselves to effective treatment through insurance products.

Risks with high-frequency and high-severity, such as hurricanes and floods in exposed areas, are candidates for various forms of risk securitization.

Risk Management Goes Real Time

Douglas McKibben, 52J, SYM12, 6-11 October 2002



Risk scenarios

Before purchasing insurance to transfer operational risk, management must evaluate:

- Level of risk the company can reasonably assume on an annual basis without severely impacting earnings
- Retention or transfer of frequency (low-impact, high-probability risks) vs. severity (high-impact, low-probability risks)
- Terms and conditions of the coverage available
- Price of insurance relative to the potential losses
- Financial strength and stability of possible insurers

© 2002 GartnerG2

Dynamic: Like liquidity or investment management, risk management requires a policy for setting portfolio targets and risk limits.

This necessitates a comprehensive view of enterprise exposures to: 1) enable offsetting positions; 2) identify growth opportunities for high risk-adjusted returns; and 3) diversify risks (protect downside).

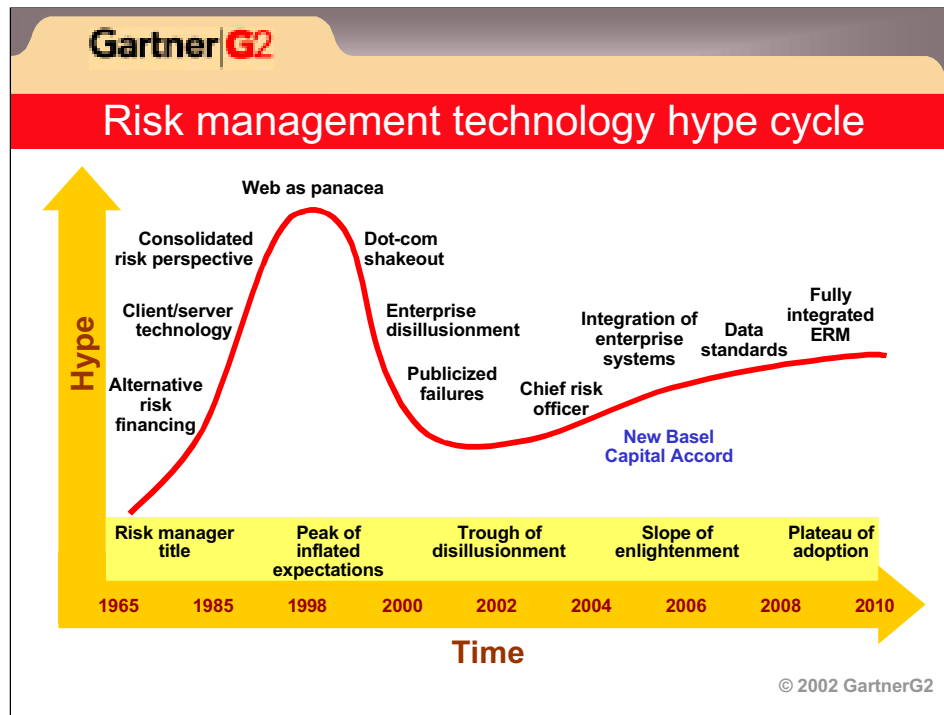
Determine the level of risk your company can reasonably assume on an annual basis without severely impacting earnings. Transfer undesirable risks to the secondary market to increase risk-generation capacity, and purchase desirable risk that cannot be generated internally.

Determine the retention of frequency (low-impact, high-probability) versus severity (high-impact, low-probability).

Insurance is historically the way for organizations to transfer or finance risks that cannot be otherwise mitigated or managed to an acceptable level. But there are limited insurance products for operational risk and traditional insurance products developed on loss history projected into the future and adjusted for catastrophic events. More products will emerge with data accumulation and sharing.

Risk Management Goes Real Time

Douglas McKibben, 52J, SYM12, 6-11 October 2002



Dynamic: Risk management is nearing the slope of enlightenment.

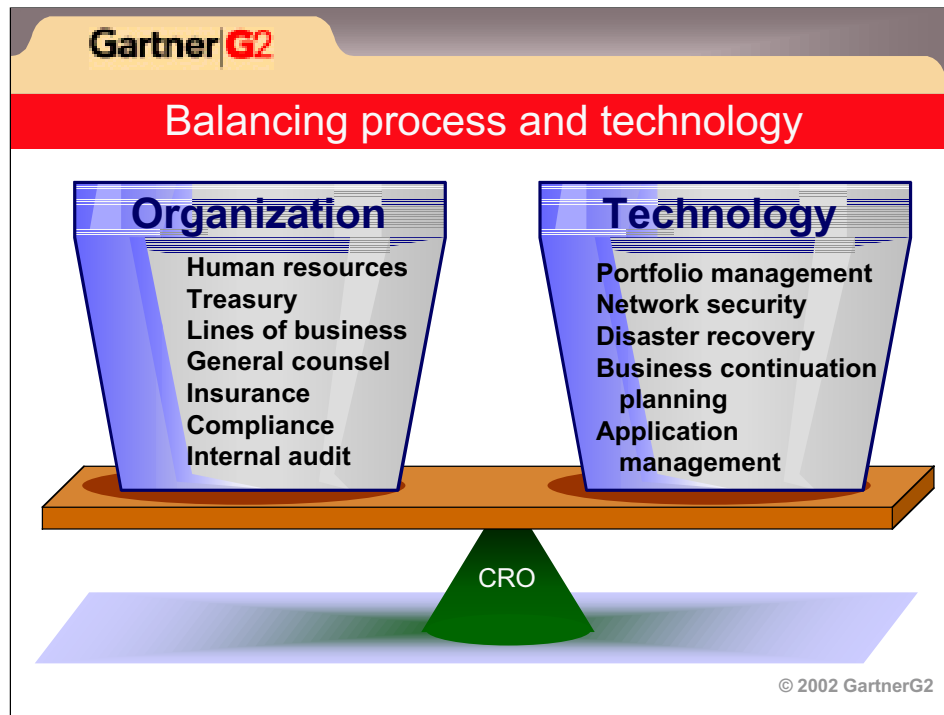
With the advent of the Web, enterprise risk management (ERM) was supposed to take off as the "next big thing." But the hype has exceeded the reality. While the Web is an enabling technology, it is not a "silver bullet."

ERM and e-commerce are both process-based initiatives. These real-time initiatives depend on integrated processes and shared, standardized data. But integration and automation should not be considered as just enablers of faster processes. The objective is productivity enhancement and simultaneous rather than sequential sharing of information. Linking bad processes will only result in faster bad processes.

Like e-commerce, ERM crosses internal lines of business and requires an executive with overarching authority. Currently, the chief risk officer (CRO) is most common at financial institutions and energy companies that have complex risk profiles. But even there, ERM initiatives have misfired, generally because of cultural inflexibility, a lack of an integrated system for collecting and reporting risk information, or because the CRO was not invested with sufficient authority.

Risk Management Goes Real Time

Douglas McKibben, 52J, SYM12, 6-11 October 2002



Prediction: ERM will be the norm by 2010.

The need to provide risk transparency for boards of directors, regulators and equity analysts will require executive-level leadership to manage risk across business units and integrate financial techniques with organizational practices and processes. The job of the CRO is a balancing act—balancing business requirements against technical capabilities, balancing risk portfolios, and balancing the cost of risk exposure against the cost of mitigation or acceptance.

The primary operational risk assessment should be shifted from the internal audit staff to the business unit creating and managing the risk. The manager of this unit is in a better position to understand and influence the range of risks. Operational audits should then include a review of the management decision process, as well as internal controls. Integrating risk assessment into business unit planning will place accountability with the line manager and requires and promotes common risk management processes. Web-based applications that permit risk information to be shared across the organization will support this process.

Continuing regulatory pressure including the New Basel Capital Accord plus the emergence of data standards and Web-based integration will result in ERM being broadly accepted by 2010.

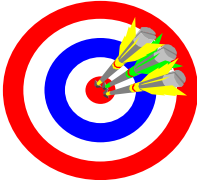
Risk Management Goes Real Time

Douglas McKibben, 52J, SYM12, 6-11 October 2002

Gartner | **G2**

Recommendations

- Start now to establish an enterprisewide approach to risk management before attempting to measure operational risk.
 - Identify the data needed.
 - Create a cost-effective plan to collect data.
 - Design an approach to measure risk.
- Identify interdependencies across lines of business.
- Obtain interpretative, operational risk expertise from other institutions, industry groups and expert sources.



© 2002 GartnerG2

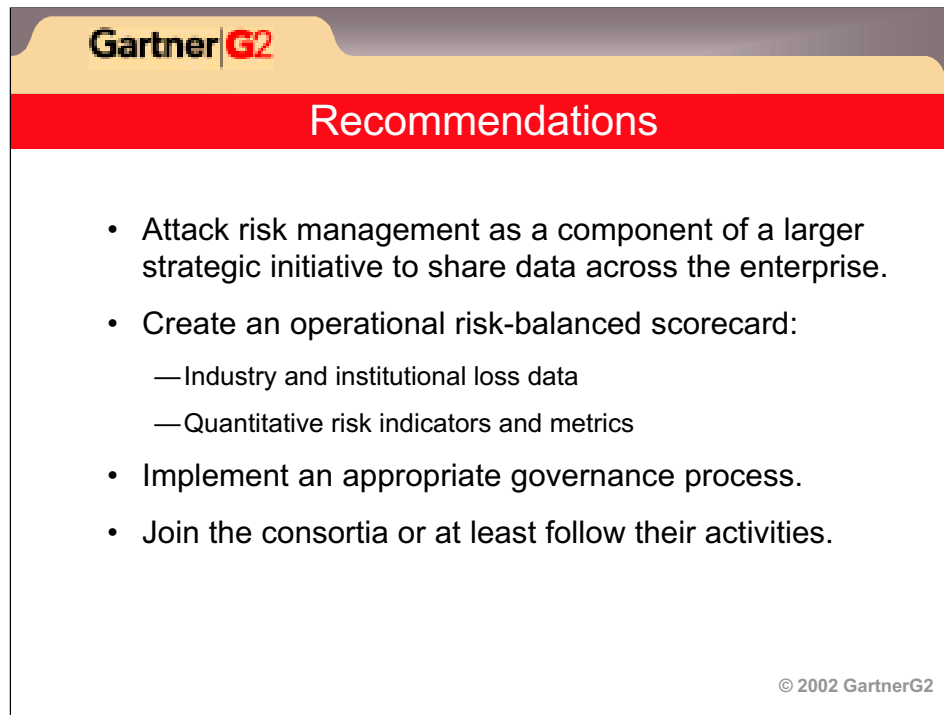
Recommendation: Start your ERM initiative now.

Establish executive-level leadership to identify risk components and integrate the risk management process across business units. Create a consistent internal understanding of the definitions, strategies, investments and processes necessary for ERM. Depending on the complexity and breadth of risk exposures, it may be desirable to create a CRO position to give fulltime attention to these activities.

Leverage external sources of information and expertise to address operational risk. Historic information—particularly that based on the limited experiences of a single enterprise—may be an insufficient indicator of future exposures. For example, the organization's past risk profile and loss experience probably will provide little understanding of the risks related to establishing an e-business channel.

Risk Management Goes Real Time

Douglas McKibben, 52J, SYM12, 6-11 October 2002



The slide features the Gartner G2 logo in the top left corner. A red horizontal bar with the word "Recommendations" in white text spans the width of the slide. Below this bar, a list of four bullet points is presented. The first bullet point is "Attack risk management as a component of a larger strategic initiative to share data across the enterprise." The second bullet point is "Create an operational risk-balanced scorecard:", followed by two sub-bullets: "— Industry and institutional loss data" and "— Quantitative risk indicators and metrics". The third bullet point is "Implement an appropriate governance process." The fourth bullet point is "Join the consortia or at least follow their activities." In the bottom right corner of the slide, the text "© 2002 GartnerG2" is visible.

Recommendation: Make business units accountable for risk.

Create a well-designed data model for collecting and understanding risk information. Assure that business and technology work together to develop a solution that fits with overall organizational and process requirements for granular data and timely performance. Participate in industry initiatives to share operational risk incident information and, where necessary, employ the specialized expertise of third parties to source and interpret risk data. Leverage insurance relationships to understand risk and evaluate measurement methods better.

Integrate risk assessment into business unit planning. Require line managers to manage risk levels and use loss and incident information to allocated economic capital to business units based on their risk profiles. Monitor this information on a real-time basis and in aggregate to provide insight into emerging trends.