# Regulatory Revolution Risks Civil War

Tim Leech

Over the last five years, the Basel Committee on Banking Supervision has been increasingly concerned with ensuring that financial institutions manage operational risk properly. Several working papers, the prominence of operational risk in the proposed changes to the Capital Accord, and an emerging set of best practices for operational risk management all contribute to, and reflect, this revolution. At the same time, financial institutions find it increasingly difficult to shift from their former management structures to ones that better meet the guidelines. The transition is a difficult one—more so for some areas in some institutions than others. This paper examines the different types of groups affected by the changes, and looks at how their interrelationships impact on the process. Further, it offers some techniques for facilitating the transition to the new world of operational risk management.

The Basel Committee on Banking Supervision's paper (BCBS 1998), entitled "Framework for Internal Control Systems in Banking Organizations," launched a revolution in risk-management thinking. The paper proposed that banks' boards of directors (the board) be held responsible by their regulators for "understanding the major risks run by the bank, setting acceptable levels for these risks and ensuring that senior management takes the steps necessary to identify, measure, monitor and control these risks." Further, it suggested that senior management be held accountable for "developing processes that identify, measure, monitor and control risks incurred by the bank."

Put simply, the BCBS recommends that banks adopt an integrated, holistic approach to enterprise risk and assurance management by eschewing traditional "silo-based" approaches to risk and assurance. Major governance studies in the United States, the United Kingdom, Canada and Europe confirm the need to find better approaches to governance.

Given the numerous, heavily entrenched risk management silos that must integrate their efforts and data to make these directives a reality, the BCBS may have also wittingly or unwittingly launched a protracted civil war among the numerous risk-management factions. The high-profile governance failures of, among others, Enron, Allied Bank, Barings, NatWest and Long Term Capital Management, highlight the pressing need to integrate and unify risk-management silos and factions as quickly as possible.

Taking such a stance is supported by research done by, among others, McKinsey (2000), Miccolis and Shah (2000), CFO Research Services (2002), Miccolis et al. (2001), the Conference Board of Canada (2001), and the Economist Intelligence Unit (2001). The findings suggest that if disparate, risk-management silos can be unified under the banner of integrated, enterprise risk management, the spoils of victory will be increased shareholder confidence and financial returns.



*This article appeared in Vol 5, No. 2 Algo Research Quarterly Magazine Summer 2002.*

This article explores some of the barriers that need to be overcome in order to achieve success. It then introduces potential tools and strategies to reduce the length and severity of possible conflicts between the various factions.

## Risk-management silos

Figure 1 shows the various risk-management silos involved. All of them play important roles in generating and storing information necessary for holistic, integrated enterprise risk and assurance management. Unfortunately, the inhabitants of the various silos often speak different languages and hoard their caches of risk data in different formats and locales. Either they prefer not to communicate with other risk-management silos or, when they do try, they have difficulty communicating effectively. In addition, corporate reward systems often provide tangible incentives to keep critical data on risk status concealed.

The silo-based approach to risk management has evolved over many decades and has deep roots. Understandably, change may not come easily and may even be fiercely resisted. Some of the battles that will have to be fought over the next decade to actualize fully the new BIS II operational risk directives will be played out among the following:

- Senior management vs. the regulators
- Senior management vs. the board
- Disclosurites (those prepared to tell all) vs. the Legalites (those who prefer to minimize disclosure and legal liability)
- Work units vs. everyone
- Old School Quals who inspect, assess, audit, and report on control adequacy) vs. the New School Quals (who facilitate risk and control analysis, train work units, validate reliability of risk status data produced by work units)
- Quants (quantitative operational risk management practitioners) vs. Quals (qualitative risk-management practitioners)
- Quals vs. the Qual-Quants (a hybrid crossbreed that wants to integrate qualitative and quantitative risk management approaches).

Unification and integration of risk-management silos, and the elevation of Qual-Quants, will be necessary to meet the expectations of financial sector regulators and, most importantly, to get on with the business of restoring shareholder confidence in a post-Enron world.

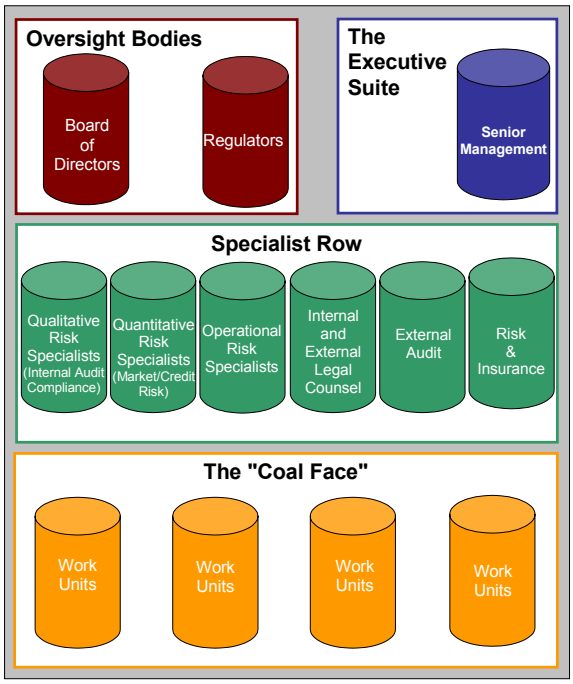


**Figure 1:** Risk-management silos

### Senior management vs. regulators

The BCBS has made it very clear that bank regulators need to be evaluating the overall quality of the risk-management systems developed and maintained by management and boards. Organizations with effective operational risk-management systems will be rewarded with lower capital requirements; reduced regulatory attention; and, potentially, reduced deposit insurance



*This article appeared in Vol 5, No. 2 Algo Research Quarterly Magazine Summer 2002.*

premiums. Organizations with weaker operational risk-management systems will be required to have higher levels of capital than their more risk-aware peers; may be charged higher deposit insurance; and will attract more regulatory scrutiny and resources. This is the good news!

The bad news is that improved systems of risk management in banks will provide their regulators with far more, far better, information on the true state of residual risk in each bank. Acting on this information may cause bank regulators to intervene and question areas of significant residual risk that were previously hidden or obscured. Regulators may take severe remedial action in situations that were previously out of sight and out of mind by using more traditional, ineffective, and secretive silo-based approaches to risk management and reporting. The resulting tensions may set the stage for an ongoing battle between these two camps.

**Senior management vs. the board**

In a perfect world, the goals of senior management and the board align. Full disclosure of the risk status to the board is fostered and rewarded. Unfortunately, in some companies, the personal aims of management conflict with the best interests of the company's shareholders and the board (e.g., Enron). Selective disclosure of the true state of risk to the board may have become a way of life. Highly edited and censored reporting of risks to the board is sometimes fostered and directed by domineering CEOs and CFOs. The absence of an executive with direct accountability for the quality of board disclosure on risk status, such as a Chief Risk Officer (CRO), compounds this problem.

Integrated enterprise risk-management systems increase the quantity and quality of information on the true state of risk to the board. Unfortunately, some boards have shown a marked tendency to not want to know about certain risk taking activities in the organization. The main reason for this behaviour is simple: once there is evidence that information on specific risks have been presented to the board, board members have a difficult time advancing the "plausible deniability" defence (BCBS 2001a).

On the other hand, some boards are deliberately buried by an avalanche of information from senior management. Important information on significant risks that have been accepted is obscured by the sheer magnitude of data presented, mainly related to insignificant issues.

The stringent new requirements from the BCBS related to the responsibility of boards to be aware of the significant risks sets the stage for increased friction in the future between senior management and their boards. This may be especially true in cases where senior management has been highly selective in terms of what they have been communicating to their boards concerning risk status.

**Disclosurites vs. Legalites**

Effective risk management requires documented analysis and assessment of the current state of risks, controls and residual risk. Residual risk is defined as the level of risk remaining after taking account of existing controls and other risk mitigators. Conscious decisions from executives and an organization's board of directors on the acceptability of significant residual risks are preferred over unconscious risk acceptance not attributable to any individual or group.

To achieve a "Very Effective Risk Management" grade from regulators, most organizations must radically increase the quantity and quality of formalized risk- and control-analysis work being done at all levels and in all areas. They will also have to adopt processes and tools capable of producing reliable, real-time, consolidated reports on residual risk status related to all kinds of risks and business objectives.

The overriding goal of these new systems and processes should be consensus on appropriate levels of residual risk by the board, and its communication to staff at every level of the organization. This enterprise risk-management goal is also referred to as determining and monitoring an organization's "risk appetite."



*This article appeared in Vol 5, No. 2 Algo Research Quarterly Magazine Summer 2002.*

By definition, true enterprise risk-management advocates are, to varying degrees, Disclosurites: people who believe that the organization will be better served if decisions by senior management and the board on significant risks are made consciously, with reliable and appropriate documentation. Unfortunately, this approach can also entail explicitly agreeing on the level of acceptability of the following:

- tolerable illegality
- contract violations with customers and suppliers
- safety breakdowns
- regulatory infractions
- deceptive disclosure in annual reports
- substandard products and services.

Enter the Legalites who are generally lawyers, both internal and external, that are trained and paid to protect, defend and enhance their client's legal position. In general, the disclosure of risk-acceptance decisions and the basis for those decisions increase the firm's exposure to civil and criminal liability. Obtaining tangible evidence of the basis used by management to evaluate the acceptability of residual risk helps prosecutors and plaintiffs establish mens rea, that is, whether there was conscious prior intent and knowledge on the part of senior management and the board related to the residual risk status of various risks the organization faces.

The law requires that organizations be able to demonstrate that they are exercising due diligence; that is, taking reasonable steps to avoid committing an offence. Here, it means taking steps to identify and manage risks. Unfortunately, hindsight often makes it easy to see that the precautions taken were inadequate. Since the availability of such information may strengthen a plaintiff's case against an organization, the transparency required to make effective risk-management decisions creates friction between Disclosurites and Legalites.

This friction is greatest in countries with a highly litigious culture. The more incentive there is to litigate and prosecute when corporate risk and control governance systems fail, the more reason for the plaintiff or prosecutor to seek evidence of criminal intent on the part of management or the board. The more effective the enterprise risk-management system, the more the documentation regarding the level of precautions an organization decides is needed. Further, the more litigious a country, the more incentives there are, in the absence of strong countervailing forces, to prefer the less-than transparent approaches to risk management afforded by a silo-based environment. In such countries, legislators and courts may have to intervene to ensure that companies are not rationally precluded from doing what is required to better manage risk of all types.

**Work units vs. everyone**

Work units are charged with a plethora of duties. They have to deliver products and services, produce profits, minimize costs, obey laws, comply with senior management and board mandates, and generally keep the company running and solvent. In many organizations, programs such as Management By Objective, Total Quality Management and Six Sigma, come and go like the tide, and often before any tangible benefits are realized. In some companies, the level of cynicism in work units regarding senior management's fad of the month runs high.

Better risk management requires work units to demonstrate that they are investing time and effort in formal risk and control analysis. This new work effort takes time away from current, pressing priorities mandated by senior executives. The long-run benefits and payback from more formal risk management must be taken on faith, in the face of short-term pain and an investment of time and other resources.

In some organizations, the corporate culture, which is "shoot the bearer of bad news," is not conducive to sound risk management. Whistleblowers, if not fired, are chastised or relegated to jobs that neutralize or gag



*This article appeared in Vol 5, No. 2 Algo Research Quarterly Magazine Summer 2002.*

them. As organizations begin to launch enterprise-wide operational risk programs, work units may be flooded with requests from head office Quants and Quals for both time and data to satisfy these new requirements.

As work units begin to disclose all that they know about risk, the Legalites may descend on them and castigate them for their candid, public admissions on sensitive topics. Disclosure of the true state of risk may cost management and staff in the work units their bonus and get people fired. Management staff in the work units may be held accountable by senior management and the board, and may even be required to justify their risk-taking decisions.

Some of the risk information disclosed by work units may cause an organization's external auditors to demand higher fees to complete additional work. Disclosure may also negatively affect financial statements and cause share price to drop, which is bad tidings for the board and shareholders alike. Public affairs personnel may have to be enlisted to assist with damage control in light of all the dirty corporate linen being aired. Regulators may respond to disclosures of risk acceptance with fines, sanctions and even closures. Understandably, the common view in work units is that full disclosure of risks is a potentially dangerous and costly undertaking.

The use of sophisticated, operational risk-management evaluation systems may also include developing risk-adjustment factors for the capital employed by work units that take into account the true status of risk and/or the quality of a business unit's risk-management process. Depending on how these factors are developed, work units that appeared highly profitable before these tools were employed, may see their risk-adjusted profits and return on capital indices downgraded. In the absence of strong justification and tangible incentives to adopt this new approach, work units may see increasing the amount of analysis and disclosure of residual risk status as a no-win proposition.

**Old-school Quals vs. new-school Quals**

Old-school qualitative risk-management practitioners (OSQs), such as internal auditors in organizations where the internal audit department is still similar to the inspection department of yesteryear, will find the transition to this new world very painful. The focus of the new enterprise-wide and operational risk-management regimes are on raising the overall quality of enterprise risk-management and assurance systems.

Old-style audit approaches—where the auditor is the primary risk and control inspector, analyst, and reporter, and where audit reports are collections of audit findings on specific issues or business units—have retarded the improvement of risk and control self-assessment systems by discouraging work units from learning the skills to assess and report on control and risk themselves. Work units may well wonder why it is necessary to go to the trouble and effort of formally assessing risk if someone else is going to assess it and then determine what to do about it.

New-school Quals (NSQs) actively and aggressively promote the use of risk and control self-assessment in work units. They do so by:

- playing a leadership role
- promoting risk and control assessment skills training for work units and senior management
- promoting the introduction of integrated enterprise risk and assurance databases
- introducing the use and benefits of risk source and control models to their organizations, and
- verifying quality assurance information on risk status produced by work units.



*This article appeared in Vol 5, No. 2 Algo Research Quarterly Magazine Summer 2002.*

The BCBS operational risk reforms may increase the divisions and rifts between these two factions by highlighting the deficiencies of the approaches and tools used by OSQs. Some in this group have indicated by actions that death is preferable to moving to the new risk and assurance approaches advocated by NSQs. In response, some of the latter are eager to identify and expose the deficiencies of the former in an attempt to rid their organizations of them.

**Quants vs. Quals**

The Basel Committee paper (BCBS 2001b), "Sound Practices for the Management and Supervision of Operational Risk," provides an excellent summary of one of the key issues in paragraph 80:

> Many leading financial institutions have attempted to supplement statistical estimates of operational risk capital with qualitative assessments of a bank's operational risk exposure, including in particular an evaluation of the risk management and control environment. While largely based on judgment (vs. statistical analysis of actual or assumed loss distributions), such qualitative assessments typically are translated into a quantitative metric that can be incorporated into the bank's risk-management process. Over time, the link between statistically based measures and qualitative factors is likely to become tighter as banks study the relationships between actual historical loss experience and judgment-based risk indicators.

In short, it suggests the need to integrate qualitative and quantitative risk-management approaches and tools.

Quals have been around for decades under a range of discriptors, including Inspection Department and Internal Audit. In general, Quals pay only limited attention to the actual performance and loss events produced by various control design combinations in use in their client organizations. They pay even less attention to loss event statistics being generated outside of the business by similar organizations. Quals have relied instead on subjective judgments of what they believe constitutes adequate and effective control management. All too often, the risk/control assessments results they report are based on the dangerous assumption that following corporate policy always produces good results.

Quals routinely do two things that compound this problem: they make recommendations to change control systems without knowing the performance achieved by the current control process; or, in most cases, measuring the change in process reliability caused by the implementation of their audit recommendations. They generally work without disclosing to their clients the underlying control models that govern and drive their thinking and recommendations. Too, they spend virtually no resources to validate the predictive reliability of the implicit or explicit control models they use.

Since Quals have rarely applied much actuarial or statistical rigour to their work, banks must recruit Quants from other risk areas in order to manage operational risk. Quants, turning their attention to the much broader area of operational risk management, begin with what they know best: quantitative analysis. This requires the collection and statistical analysis of internal and external operational risk data to provide input to standard methods and tools. Some of the tools Quants use are:

- Extreme value theorem
- Causal modelling analysis
- Delta EVT
- Statistical actuarial modelling
- Monte Carlo simulations
- Bayesian networks and methods
- Error propagation
- Risk-adjusted return on capital
- Value at risk.



*This article appeared in Vol 5, No. 2 Algo Research Quarterly Magazine Summer 2002.*

Much of their work focuses on the analysis of history, both internal and external, to understand patterns and predict the future.

Quantitative tools and approaches are often foreign to Quals who generally rely on audit programs and implicit command/control paradigm control models that have not been empirically validated. The use of what is termed "direct controls" such as supervisory reviews and approvals, passwords, reconciliations, documented corporate policy statements and rules are still considered by many of them as the key attributes of an effective risk- and control-management framework.

Friction, misunderstanding and conflict between these two groups are emerging and may increase. A recent effort to have a Quant address a conference of Quals at an international risk and control self-assessment conference elicited low speaker ratings. The Qual's general response was that the Quant's presentation was irrelevant, at best, and incomprehensible, at worst.

Similarly, Quants show little tolerance of what they perceive as a lack of intellectual rigour and application of scientific and actuarial principles by Quals in their approach to risk and control assessment. Quants generally ignore the efforts of internal audit departments and concentrate instead on populating databases with "real data." These are, specifically, internal and external loss event and process-performance statistics that can be tracked, analysed and extrapolated using analytical tools that are familiar to them. Given the entrenched behaviour of both camps, it may take some years for their different perspectives on the world of risk management to converge.

**Quals vs. Qual-Quants**

A hybrid breed of risk and assurance specialist is emerging—Qual-Quants. These professionals advocate the use and integration of the newest qualitative and quantitative risk-management approaches and tools to manage better all types of risk. For example, they promote studying the correlation between various combinations of controls (i.e., the control design) and their effect in terms of loss-event statistics and key performance indicators.

They also advocate the use of activity-based costing principles to increase the visibility on the cost of control relative to the potential impact of the risks being mitigated. They believe that when senior management sees that more formal and rigorous risk assessment results in better overall performance, more resources will be devoted to making true enterprise-wide risk management a reality.

Qual-Quants advocate using enterprise risk and assurance database technology to track and report the state of risk and control on a real-time basis. The predictive ability of the control and risk models they use to evaluate and report various combinations of control elements is continuously and critically assessed in light of actual performance/loss event results. Recommendations by specialist assurance groups, when implemented by work units and/or senior management, are monitored to determine if they actually improve performance and/or reduce losses.

Qual-Quants are a foreign notion to OSQs and NSQs alike, and both camps regard them with suspicion. Open warfare between Qual-Quants and OSQs is possible because the tools used by the former are often engaged to expose publicly that OSQs add little tangible value relative to their cost, and may even be seriously harming the welfare of the firm. The fact that many of the organizations that have suffered major failures have had traditional internal audit groups adds weight to their findings.

Friction may also emerge between NSQs and the Qual-Quants, but experience suggests that many NSQs can be converted into Qual- Quants. Unfortunately, not everyone will make the transition to this higher level of risk-assessment rigour and performance visibility.



*This article appeared in Vol 5, No. 2 Algo Research Quarterly Magazine Summer 2002.*

## Silo-busting techniques

In light of the many formidable barriers to implementing holistic, integrated enterprise-wide risk management, one might question whether the conflicts of interest among the feuding risk-management silos can be resolved.

Forward-looking practitioners of all stripes in this field have been wrestling with these significant structural challenges and continue to search for new tools and techniques to overcome the barriers. An inventory of some of the most promising strategies follows.

**Appoint a Chief Risk Officer or equivalent**

First, organizations may wish to consider formally appointing a Chief Risk Officer (CRO) or a risk unit to report to senior management and the board on the quality of risk-management processes already in place. Second, this person or unit will report on the consolidated residual risk status across the entire organization. To meet this type of mandate, this individual or unit will have to take steps to break down the existing risk-management silos to produce and extract efficiently the information necessary to provide an integrated, holistic picture of the true state of risk on a real time basis. If this mandate is not assigned to a CRO, an alternative is to require the General Auditor/SVP Internal Audit to provide this information to senior executives and the board.

**Modify reward systems**

Only with proper incentives, or disincentives, can the employees of any organization embrace a risk-aware culture. Incentives to collect data, analyse risk and controls, cooperate across departments or functional roles, and adopt management initiatives are crucial.

The BCBS recommendations on operational risk management practices implicitly recognize that there are major barriers to banks adopting the new approach to risk management and reporting. This is apparent from their proposal to link minimum capital requirements to a regulator's assessment of the quality of a bank's operational risk-management system. They are proposing significant financial rewards and consequences to stimulate compliance efforts.

Some financial regulators have also suggested linking deposit insurance premiums to the quality of a bank's risk-management processes. This would be an additional incentive to banks to tackle the difficult job of adopting better, more integrated, enterprise-wide risk management practices. Similar incentives do not currently exist in other industry sectors.

If organizations are to make to make this transition successfully, in addition to regulatory incentives, boards must also take steps to ensure that senior management incorporate appropriate incentives and disincentives in their systems to encourage candid and reliable disclosure of the true state of risk. Work units will also need tangible incentives and practical reasons to invest the resources necessary for more rigorous risk and control management.

Internal audit departments may wish to consider rewarding work units that provide reliable and candid disclosure of the true state of risk with good reliability ratings on disclosure, even in cases where the information disclosed by the work unit suggests significant risks are being taken. Work units that show little evidence of effective risk-management systems could be encouraged towards compliance by having poor "risk fitness" scores reported to senior management and the board. The new professional standards of internal auditing, effective January 1, 2002, support this transition.

**Adopt a common language of risk**

To support a risk-aware culture, a common language is critical. If everyone learns to express risk, control, mitigation and management issues in the same language, misunderstandings can be avoided.



*This article appeared in Vol 5, No. 2 Algo Research Quarterly Magazine Summer 2002.*

Furthermore, policies can be more easily compared, evaluated, adapted and adopted.

Recent developments are slowly moving the world of risk management toward common definitions of the terms “risk management” and “control.” The BCBS Working Paper on the Regulatory Treatment of Operational Risk (BCBS 2001b), has adopted a common industry definition for operational risk, namely, “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.”

Numerous bodies worldwide have proposed definitions for the term control. One that appears to be meeting with a fair measure of acceptance was proposed by the Canadian Institute of Chartered Accountants (CICA) in their publication entitled Guidance on Control (CICA 1995). The CICA defines control as “those elements of an organization (including its resources, systems, processes, culture, structure and tasks) that, taken together, support people in the achievement of the organization’s objectives.”

To demystify risk management and support enterprise-wide training CARD®*decisions* Inc., a Canadian company specializing in risk and control training and technology has developed and uses the terminology shown in Figure 2.

An Institute of Internal Auditors Research Foundation study entitled Enterprise Risk Management: Trends and Emerging Practices (Miccolis et al. 2001) defines Enterprise Risk Management as: “A rigorous and coordinated approach to assessing and responding to all risks that affect the achievement of an organization’s strategic and financial objectives. This includes both upside and downside risks.” These definitions are understandable and largely consistent with emerging international views on the definition of risk and control management. A common risk language is a primary building block for a sustainable enterprise risk initiative.

**Implement enterprise risk-management software**

Enterprise risk-management software, including information dissemination, data collection, work flow systems, and the like, is another important tool in breaking down silos. However, its contribution to other techniques is also significant.

Two key BCBS requirements relate to developing and maintaining an enterprise-wide information system that identifies, measures and reports on the state of risk to senior management and the board. To be effective, except in very small organizations, it will require using a computerized system to capture, analyse, monitor, validate and report on the status of risk and control.

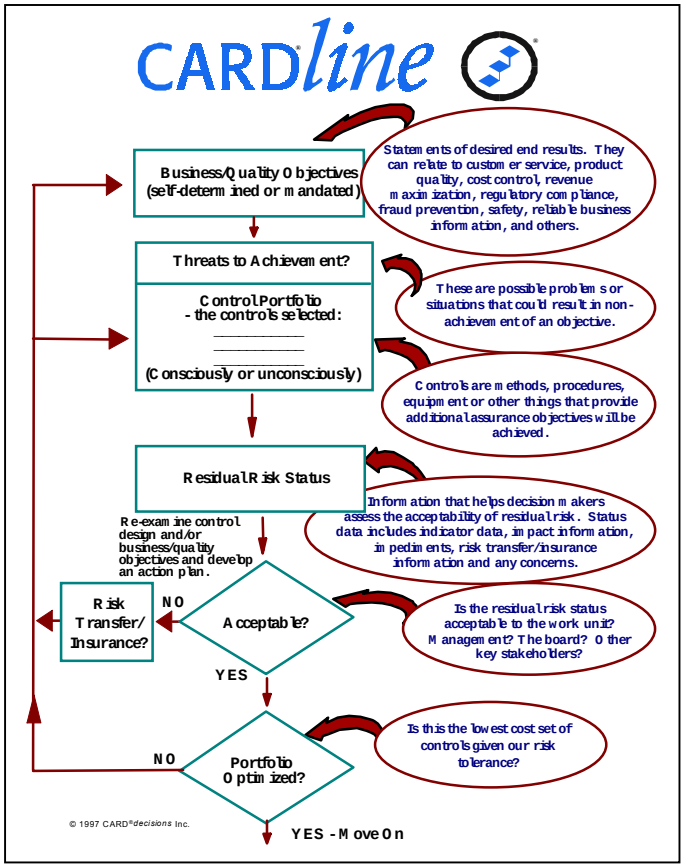


**Figure 2**: CARD®*decisions'* enterprise risk-management terminology



*This article appeared in Vol 5, No. 2 Algo Research Quarterly Magazine Summer 2002.*

A case in point is ERAM software, which can be used to:

- assign responsibility
- gather data
- measure and report on the tangible benefits of using more formal approaches to risk and control
- foster the use of common approaches and terminology to assess and report on risk status, and
- to validate and report on the processes used to generate information on risk status to senior executives and the board.

Satisfying fully the proposed regulatory requirements will require the use of one system for gathering, analysing, monitoring and validating risk and control data. Another system can be set up to provide statistical analysis and calculation capabilities using both internal and external loss event information. Over the next few years, fully integrated, holistic, quantitative/qualitative enterprise-wide risk and assurance software systems will emerge to meet these needs.

**Provide risk-awareness training to all staff**

Risk and control assessment must become routine practice at all levels of an organization to ensure the sustainability of enterprise risk initiatives. This approach requires an investment in training if the new requirements are to add real value and improve performance.

New methods use computer-based training modules to introduce risk and control management skills quickly and cost-efficiently to large numbers of employees operating in different countries and speaking different languages. Great strides have been made to develop easy to understand tools and approaches to train staff in the core fundamentals of good risk management.

## Whither the future of operational risk?

BCBS reforms have launched a revolution in risk management that highlights the deficiencies and inefficiencies of traditional approaches to risk management. It also intensifies the conflict between all of the risk-management silos identified earlier. Those organizations that succeed in breaking down the barriers and unifying the efforts of the inhabitants of these silos will reap the benefits envisioned by BCBS and, more importantly, will realize the significant economic and societal benefits that flow from high performing, well-run and well-governed organizations.

Conversely, those organizations that do not succeed in overcoming the considerable inefficiencies and dangers of the traditional silo-based approach to risk management will continue to risk repeating the painful experiences of Enron, Allied Bank, NatWest, Long Term Capital Management and others.

Only time will tell which of the existing risk-management silos, if any, are prepared to fight, perhaps to the death, rather than join with the other groups to help in achieving the benefits of integrated, enterprise-wide risk and assurance management.

## Endnote

1. Plausible deniability will be a key element of the defence position presented by the Enron Board of Directors.

## References

Basel Committee on Banking Supervision, 1998, “Framework for Internal Control Systems in Banking Organizations,” Basel Committee on Banking Supervision, September,www.bis.org/ publ/bcbs40.htm.

Basel Committee on Banking Supervision, 2001a, “Working Paper on the Regulatory Treatment of Operational Risk,” Basel Committee on Banking Supervision, September, ww.bis.org/publ/bcbs_wp8.htm.



*This article appeared in Vol 5, No. 2 Algo Research Quarterly Magazine Summer 2002.*

Basel Committee on Banking Supervision, 2001b, "Sound Practices for the Management and Supervision of Operational Risk," Basel Committee on Banking Supervision, December, www.bis.org/publ/bcbs86.htm.

CFO Research Services, 2002, "Strategic Risk Management: New Disciplines, New Opportunities," New York, NY: CFO Publishing Corp, March, A study, www.aon.com/about/publications/issues/2002_aon_cfo_report.jsp.

Canadian Institute of Chartered Accountants, 1995, Guidance on Control, Toronto, ON: Canadian Institute of Chartered Accountants, www.cica.ca/cica/cicawebsite.nsf/public/sgcoss_sspco8.

Conference Board of Canada, 2001, "Integrating Risk Management through a Change Management Process," Ottawa, Ontario: Conference Board of Canada, September, A research Report, www.conferenceboard.ca/contact.htm.

Economist Intelligence Unit, "Enterprise Risk Management: Implementing New Solutions," 2001, New York, NY: Economist Intelligence Unit in cooperation with MMC Enterprise Risk, A commentary, www.mmcer.com/comment/FinalExecBrief.pdf.

McKinsey & Company, 2000, "Investor Opinion Survey on Corporate Governance," McKinsey & Company, June, Article from website, www.mckinsey.com.tw/publications/organization_investor_survey.pdf.

Miccolis, J. and S. Shah, 2000, "Enterprise Risk Management: An Analytic Approach," New York, NY: A Tillinghast-Towers Perrin Monograph, January, A monograph from website, www.towers.com/towers/publications/erm/erm2000.htm.

Miccolis, J., K. Hively and B. Markley, 2001, Enterprise Risk Management: Trends and Emerging Practices, Altamonte Springs, Florida: The Institute of Internal Auditors Research Foundation with the assistance of the Conference Board of Canada, A monograph, www.theiia.org/iia/bookstore.cfm?fuseaction=product_detail&order_num=433.



*This article appeared in Vol 5, No. 2 Algo Research Quarterly Magazine Summer 2002.*