

Unlocking business value
from effective operational
risk management

A BT point of view

Why care about operational risk?

Protecting corporate assets, providing a continuous service to customers and being able to defend the organisation against attack has never been as important as it is today.

Business is more complex than ever before. Globalisation, growth in electronic business and the outsourcing of many business functions introduce more exposures. The impact of potential attacks – internal or external – natural or man made – is greater than ever before. As a result, the way organisations manage their exposure to operational risk has become an important boardroom issue.

According to recent research by BT, increased regulation is the main driver behind corporate investment in operational risk management processes and systems. However, many organisations have responded to increased regulation by taking a limited view, doing just enough to keep the regulators happy.

BT's view set out in this paper is that organisations are now realising that effective operational risk management is indeed more than just about compliance, but a tool that can improve operational efficiency and add significant shareholder value.

What is effective operational risk management (ORM)?

BT believes that operational risk should be driven for performance, an approach that leads us to define operational risk management as a programme of enterprise wide activities that...

“...operate within a targeted level of risk parameters, and in full compliance with regulatory and corporate guidelines, aligned with business objectives, maximising operational performance while simultaneously minimising cost...”

The risk management group of the Basel Committee on banking supervision has identified that the crucial elements of an effective operational risk management framework are:

- Clear strategies and oversight by the board of directors and senior management
- A strong operational risk and internal control culture (including, among other things, clear lines of responsibility and segregation of duties)
- Effective internal reporting and contingency planning.

A cursory sweep of journals and publications covering operational risk management topics clearly shows that it is having the greatest impact on financial services organisations. Indeed, according to a panel of chief risk officers at a recent conference, the level of regulation in financial markets has reached saturation point. However, other sectors are following the lead taken by the financial institutions and beginning to implement their own operational risk management frameworks. While all sectors have to comply with Sarbanes-Oxley, data protection acts and other international and domestic standards, the other sectors that appear to be most proactive in their response are the pharmaceutical and government sectors.

The cost of compliance – “Y2K without the end date”?

The cost to financial institutions of implementing operational risk management has prompted a number of commentators to liken its impact to that of Y2K – but without the end date. For BT, this highlights the urgent need to optimise company wide efficiencies in the risk management process, as well as to view operational risk management as an opportunity to build shareholder value instead of just an unavoidable cost of doing business.

And the problem is very real; recently in London (October 2005), Digby Jones, Director General of the UK’s Confederation of British Industry (CBI) stated that companies in the US were each spending an average of \$5 million per annum just to comply with Sarbanes-Oxley. Research from McKinsey suggests that while the cost could range from \$100 million to \$250 million for larger banks, much of this investment would be required to upgrade their systems to keep pace with improvements in risk management techniques.

A speech last year from the group technology officer of Barclays Bank gives an insight into the cost of compliance. According to CTO Kevin Lloyd, 40% of Barclays’ IT investment spending is on Basel II and Sarbanes-Oxley (SOX) compliance programmes.

Once Basel II and SOX programmes are completed, another major expense is on the horizon. The European Commission’s forthcoming financial services directive (MiFID) is being touted as costing financial services institutions up to \$6 billion in compliance costs.

Evidence from other industry sectors suggests that while not as high as in financial services, the cost of implementing and deploying operational risk management is just as much an issue. BT research has found that among European pharmaceutical companies, the IT cost of compliance is a key issue for senior management.

Organisations that fail to see the bigger picture and take a limited view may indeed proceed to deploy individual risk management frameworks for each business area or each regulatory requirement, but this often leads to wasting effort and money building duplicate systems and processes in isolation.

In our view the overlap between the requirements of, for example, Basel II and Sarbanes-Oxley is quite large. An integrated approach using common frameworks to comply with multiple requirements, will enable organisations to minimise the cost burden by eliminating inefficiencies in duplicated risk management frameworks, procedures and systems.

The impact on corporate budgets is leading many organisations to think creatively about how to effectively manage and control the cost of compliance and operational risk management. Ensuring third party providers are effective in the mitigation and management of operational risk is therefore an important element in the negotiation of outsourcing and managed service contracts.

Is operational risk any different to other business risks?

Every day in the course of their usual business, banks make risk decisions about who to lend money, what securities to trade, etc. The same is true in other sectors; senior managers make decisions that involve risks – credit risks, market risks and risks that arise from publicity regarding activities that may affect the companies brand and reputation. As people face these risks every day, they have become very good at assessing and managing such exposures, putting in place people, processes and systems to manage this crucial aspect of their businesses.

However, operational risks continue to present new and different challenges. From BT’s work with corporate risk managers, it is clear that our customers have to grapple with a range of operational risks, ranging from disgruntled employees, terrorists, natural disasters around the world and so on. Other previously minor issues may take on new levels of risk in the connected world. The opportunity for a disgruntled employee to cause serious harm is greater now that employees have access to mission critical systems and data from their desktop or living room. New forms of communication have also magnified risk. The use of Instant Messaging technology between trading rooms and their customers is already causing headaches for compliance staff. And companies are beginning to track SMS messages sent from corporate mobile phones.

Organisations are increasingly realising that new processes, backed up with new technologies need to be put in place to cope with these new exposures.

A proactive approach to risk management

Risk management framework and BT risk cockpit

In BT we believe that organisations have to take a proactive approach to risk management to address operational risk. Operational risk management impacts all functions of the organisation, requiring managers to monitor a wide range of processes and procedures, from systems usage and leavers' exits to joiners' inductions and staff communications in the same way they previously monitored credit and market risks.

In our view, the skill in operational risk management is based on bringing together the data to enable the assessment and monitoring of potential risk areas and then having the mitigation processes in place to deal with them when they occur. Awareness of compliance issues and the importance to all staff of effective operational risk management needs to be embedded into corporate culture.

We recommend that organisations put in place a model and a framework that:

- Identifies, assesses and analyses risks from all relevant processes and procedures
- Has in place effective monitoring and controls to manage operational risk exposures
- Has an effective plan to limit impact or reduce likelihood as a risk/exposure develops.

BT's approach is multi-faceted, supporting comprehensive audit and management techniques with the appropriate technology tools, such as "Risk Cockpits". In BT's experience, the most effective operational risk models and frameworks will utilise a risk cockpit or dashboard to provide a single, clear view of the status of the organisation's operational risk across the whole business. Evaluating an organisation's operational risk exposure will increasingly become part of the operational due diligence process in merger and acquisition transactions.

Technology tools such as risk cockpits or dashboards automate the collation, monitoring and management of operational risk data. Previously, many of these tasks required human intervention to complete. The use of these tools significantly reduces the overall cost to the enterprise of implementing an effective operational risk management function.

A crucial feature of the most effective models is their ability to perform Intelligent Data Analysis (IDA). IDA takes learning from previous incidents of risk exposures and losses and automatically incorporates this historical data into the model to improve risk modelling and assist subsequent decision making. The use of business modelling and simulation for operational risk management is similar to the methodologies used by the aviation industry to minimise the risk of new products.

BT itself invests considerable resources to develop leading edge operational risk models and frameworks that incorporate Intelligent Data Analysis.

Operational risk management and shareholder value

The evaluation of operational risk management is becoming a factor in financial security rating agencies' appraisal processes, providing a compelling argument in support of its contribution to the creation of shareholder value. According to Moody's Investment Services Corp; "operational risk management improves the quality and stability of earnings, thereby enhancing the competitive position". Thus, not only can effective, integrated operational risk management create shareholder value through improved efficiencies, it can also reduce the organisation's cost of capital. As a result of its operational risk management strategy, Wachovia Corp, a leading US financial institution was upgraded to 'AA' rating by Moody's, making it easier and cheaper to raise capital.

For financial services companies, an effective operational risk management function can positively effect the organisations' capital adequacy requirements. Even for a relatively small US bank such as Zions Bancorp, the benefit from a reduction in capital requirement for operational risk provisions had a major impact on shareholder value, freeing up an estimated \$70 million in economic capital, which it can return to its shareholders or reinvest in its businesses.

Strategy consultants Mercer Oliver Wyman — in the context of compliance with Basel II – also stress the benefits of regarding operational risk management as a value creation opportunity. They believe that "in most cases there is a strong business case for (adopting Basel II), which outweighs implementation costs, especially for banks with large retail exposure, including regional and smaller banks, and monocline institutions in general."

Many organisations – including Fidelity and Citigroup are promoting the excellence of their operational risk management as a competitive differentiator. JP Morgan Chase expects their operational risk management programme to enhance financial performance.

Taking the key practical steps

Unsurprisingly, a professional and rigorous approach is required to deal with an area as important as operational risk management. For many organisations the choice of a methodology is the first important practical step in implementing an effective operational risk management programme.

The methodology should ideally be used as a baseline/yardstick to help measure an organisation's risk management system and hence provide steer and guidance on areas for improvement. Where no formal risk management system is in place the methodology should be used as a template to help implement a recognised risk management system.

BT's own methodology for client consulting engagements is based on the Deming Cycle (a model for continuous quality improvement). This approach is based on a number of phases which are mapped on to the Deming cycle as follows:

- **Plan:**
Identify the risks;
Calculate the risk values or levels;
Decide how the risks are to be treated;
- **Do:**
Choose the controls to mitigate the risks;
Implement the controls;
- **Check:**
Check the implementation of the controls;
- **Act:**
Put in train improvement plans to address implementation deficiencies.

Implementing this approach across an organisation should provide business executives with a high level of confidence that any company investment in operational risk management will provide real value for money.

Summary

In BT's view, the increased complexity of the business world means that organisations need to care as much about operational risk as they do about the other risks they face in the course of their business. Increasingly, managing operational risk is being seen as an opportunity to create value rather than as an exercise in keeping the regulator happy.

For BT, the operational risk management debate has moved on from applying operational risk management to meet compliance requirements focused upon operational performance to the value of effective operational risk management as an enabler of more effective business performance.

The data required for effective operational risk management systems and processes is classed by BT as real time business intelligence and is not just of value to the compliance and risk management team. This intelligence about how the business is operating on a real time basis is of considerable value to senior managers seeking to improve the overall efficiency and cost effectiveness of operations.

From BT's perspective, the business benefits of effective operational risk management are clear. Benefits include enhancing customer and shareholder confidence in the stability and success of the organisation, right through to improving operational efficiency. All of these provide a compelling argument for organisations to invest to get it right.

While for many organisations the cost of compliance can be high, organisations that see operational risk management as an opportunity to improve their business through more effective processes and systems are being rewarded by customers and shareholders alike.

External Sources used to compile this BT point of view include:

IDL European and US Financial Services and Pharmaceutical Benchmark Studies, 2005; Financial Regulation at Saturation Point, Operational Risk; The Business Case for Basel II; Computer Weekly; Moody's Investor Services Corp; The RMA journal; Operational Risk Management, Operations Council. All companies referred to in this point of view document have been quoted from these sources.

BT and operational risk management

The scale and critical nature of BT's networked IT services operations demand a world-class approach to operational risk management and BT has an established pedigree in managing complex network and IT security problems. Here are some facts about our achievements:

- BT is an acclaimed industry leader in terms of managing its own risks and has one of the best risk consultancy practices in the world.
- BT is a leader in risk related research with full-time research professionals engaged in developing BT's proprietary risk models and frameworks for use with customers and in BT's own operating businesses.
- BT has successfully completed numerous large projects which directly mitigate operational risk in various industry sectors.
- BT is developing the 'BT Risk Cockpit', which will offer customers control and visibility of their operational risks across their business. This will be designed to provide key decision makers a clear view of the status of their organisation's operational risk, measured against identified business criteria.
- BT serves 10,000 multi-site corporate customers worldwide, of which more than 3,400 are multinational companies operating in two or more countries.
- BT carries 80 per cent of all credit card transactions in the UK as part of an estimated £70bn of funds transferred each day.
- BT manages the data networks for 90 per cent of the major UK financial institutions, payment organisations and credit card companies.
- BT provides the networks that transport other high value financial transactions, such as SettleNET, in the UK.
- BT is a key contributor to the UK's Critical National Infrastructure, supplying security solutions to Government, Defence, Finance and Commercial organisations worldwide including the MoD, NHS and Emergency services.

To find out more about how BT services can help you maximise network security and drive operational efficiency, please visit:

www.bt.com/globalservices/security

contact your BT Account Manager
or alternatively call 00 800 8000 2000



Offices worldwide

BT and the 'connected world' logo are trademarks of British Telecommunications Plc.

The telecommunications services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's or its subsidiaries' respective standard terms and conditions. Nothing in this publication forms any part of any contract or is in any way an offer to contract.

© British Telecommunications plc 2005.
Registered office: 81 Newgate Street, London EC1A 7AJ.
Registered in England No. 1800000.

Designed by Unigraph Limited 22521/11/05
Printed in England.

PHME 49224