



Bringing it all together

Why Risk Management Is Never A Gamble

BT White Paper

By Dr Hannes Lubich

Head of Business Continuity,
Security and Governance Practice

Contents

Executive Summary	2
Introduction	3
Operational Risk	3
A New Landscape Of Risk	4
Customer Impact	5
The Full Cost Of Risk	6
The Death Of Innovation	7
A Balanced Risk Approach	7
Realtime Risk	8
Bottom Up Or Top Down Approaches?	8
Plan, Do, Check, Act	9
Strategic Testing	10
Responding In Realtime	10
Document Retain, Reproduce	11
Gaining Insight	12
Conclusions	12
Risk To Reward	13

Executive Summary

The world is changing fast. Rapid globalisation promises huge rewards for organisations that can integrate the best skills, infrastructure and methods that the world has to offer. Unfortunately new rewards come with new risks.

Effective operational risk management is the essential ballast for open, flexible and collaborative firms. A failure to identify and mitigate risks is tantamount to a rash gamble that leads to all kind of expensive brand damaging issues: security breaches, rogue employees, lost data, poor performance and regulatory action.

Yet paralysis remains an unwelcome by-product of risk management. Businesses are still coming to terms with the fall-out from Enron and WorldCom and many firms must avoid the trap of complying rather than innovating.

Risk aversion is equally unsustainable. Traditional controls may ostensibly protect individual operations and assets, but fail to protect the evolving business processes required to guarantee success in the global economy.

To address these issues, organisations must embrace risk management and create teams, systems and reporting models that reflect their business and the changing risk landscape. This paper looks at the key issues involved with creating a response to the evolving threats associated with networked IT systems and provides responses to emerging problems.

Introduction

Risk management is, and always has been, a fact of organisational life but the consequences and repercussions of failure now were unimaginable even ten years ago. A serious failure could, once upon a time, bring down a company. Today, the emergence of worldwide collaborative business methods means failure is no longer isolated: in fact it can shake the roots of the global economy.

Risk is headline news because organisations are shifting traditional boundaries to take advantage of globalisation. Today's risk is shared among partners and suppliers across an ever growing value chain.

Attention on risk continues to escalate. In recent times powerful new regulatory regimes have emerged, sensitive data keeps disappearing, intellectual property is stolen and a seemingly regional issue, involving sub-prime lending in the United States, turns into the threat of a global recession.

Organisations that fail to accept risk will miss out on the benefits promised by collaboration and globalisation. In the words of the Jericho Forum, a group dedicated to managing security as enterprise boundaries extend, there are growing "business demands for secure IT operations in our open, Internet-driven, globally networked world."¹

Organisations know that future success depends on flexible working, rapid response and empowered employees. They also know that open methods bring risks that could, if not managed effectively, deliver catastrophic consequences. The question for today's organisations is how to take operational risks that don't bet the existence of the business.

Operational Risk

Most people understand financial risk but organisations have become increasingly focused on another category of risk: operational risk or, in other words, the risk of losses caused by inadequate or failed internal processes relating to people, systems and external events.

The Basel Committee on Banking Supervision – a leading authority on the definition and assessment of risk in the financial industry – defines seven categories of operational risk:

- Internal fraud – where losses are caused by the inappropriate behaviour of a firm's employees;
- External fraud – which covers not only theft and robbery, but also hacking or phishing attacks conducted by people outside an organisation;
- Failures of employment practices and workplace safety measures – which may result in law suits for unfair dismissal, prosecution under anti-discrimination laws, personal injury claims and so on;
- Product and service failures – which increase the costs of warranty repairs and compensation claims and could, in extreme cases, lead to civil or criminal prosecution;
- Damage to physical assets – such as plant and buildings, for example as a result of fires, natural disasters, or terrorism;
- Systems failures – including those of computer hardware, computer software, telecommunications networks and utilities;
- Process failures of all kinds.

In part, the recent risk focus comes from legal and regulatory changes in response to executives bringing firms to their knees by failing to distinguish between responsible risk taking and irresponsible gambling.

¹ <http://www.opengroup.org/jericho/>

A New Landscape Of Risk

The benefits of convergence are well understood. Modern business processes evolve with technology and are now relying on networked applications that can be accessed on increasingly diverse forms of hardware devices, such as smartphones, BlackBerrys and PDAs.

Convergence is unleashing more significant, rapid and far-reaching changes. Information and communication technologies now play a fundamental role in managing global workforces, infrastructures and extended collaborative supply chains expected to underpin future profits.

There are four key factors emerging in the new landscape of risk: globalisation, legal and regulatory involvement, personal responsibility and loss of public trust.

Globalisation

Firms have embraced globalisation and grabbed opportunities to evolve outsourcing approaches and extend supply chains. Unfortunately rewards often bring new risks. Modern, networked organisations face a new breed of threat that, unchecked, emerges overnight and spreads rapidly across the networked world.

“The 21st century and its business models are bringing new risks and impacts that threaten the very survival of every organisation. They bring new challenges and opportunities for both continuity and risk managers, which is pushing these managers well beyond their traditional skills and continuity roots, which involved the fast replacement of IT and other facility infrastructures. They demand new skills and a new corporate risk awareness, and this is placing these professionals at the very heart of the organisation’s strategic decision making.”

ITadviser, March/April 2007 ²

Legal and Regulatory Involvement

The legal and regulatory changes on the back of the shocking collapse of Enron and WorldCom has changed organisational approaches to risk. The Sarbanes-Oxley Act (SOX), in particular, was designed to focus executive and management attention on the nature and effectiveness of measures in place to prevent process errors, security breaches and other failures.

The impact of SOX has been much broader than the American market. Globalisation means value chains have increased in length and complexity and corporations, irrespective of their base, have been forced to act. The fact is that firms must comply with the regulations of every jurisdiction in which they operate.

But SOX and other related laws are not the only reason for firms to reanalyse exposure and responses to operational risk. Accelerating globalisation is enabling new ways of working and convergence – the fusion of IT and communications – has reshaped the world’s economy to transform the way business works.

New risks are the natural corollary of new opportunities. Today, firms must respond swiftly and effectively to changes in the risk landscape – irrespective of time and geography.

Personal Responsibility

New regulations, imposing a raft of new responsibilities on senior managers, have been introduced in parallel with the emergence of new risks. Executives are no longer permitted to delegate the risk management oversight function that underpins any corporate governance framework.

The new legal focus highlights another significant impact on business risk. Organisations tend to focus on external hackers and fraudsters but cannot afford to ignore the threat from disgruntled or rogue employees with easy access to mission-critical systems and data. Employees, whether wittingly or unwittingly, can and do expose firms to attacks or, more prosaically, losses that, in recent high profile cases, have run into billions of dollars.

² http://www.nccmembership.co.uk/pooled/articles/BF_WEBART/view.asp?Q=BF_WEBART_286537

Falling Trust

In response to public concern about identity theft, legislators across the world have been tightening data protection laws. The State of California, for instance, passed a Security Breach Notification Law in 2003 to force firms to contact customers if they know, or suspect, customer personal data has been compromised. The legislation, soon followed elsewhere, applies to any organisation in the world that holds data on Californian citizens.

Such laws combined with growing media interest in identity theft leaves organisations facing a two-front assault for carelessness or negligence. A stiff fine is never welcome but a breakdown of trust leaves organisations with a battered reputation that may, ultimately, be impossible to overcome.

Consequently public and consumer trust is low as breaches become commonplace. The chronology maintained by the Privacy Rights Clearinghouse³ provides a sobering record of lapses involving hospitals, universities, retailers, government departments and almost every other kind of US organisation. The failings in other countries are also apparent. A series of lapses in British Government departments put the personal records of many millions of citizens at risk.⁴

Customer Impact

Another major problem associated with today's complex, distributed and virtualised technology environments is interrelationships. Failures often have huge knock on effects for employees, partners and customers.

The internet phone service Skype suffered a high profile outage in 2007. What was described as a 'unique set of events' exposed a dormant software flaw. The scale of the problem meant around 220 million users worldwide were left unable to make calls.⁵

Unfortunately, testing is not an exact science: there is no way an organisation can know how much testing is enough. What is clear, however, is that experience, expertise and understanding is required to identify and solve increasingly complex problems quickly – such concerns are fundamental to effective risk assessments.

Performance Issues

Another element of risk is failure to provide enough capacity to meet network demand. Staff who install new programs or, more innocently, tune into a CEO podcast, can quickly clog up a network and jeopardise the organisation's ability to handle mission critical transactions.

A survey conducted by Yankee Group in 2006 found that the typical multinational loses more than one million hours of employee productivity a year. In certain industries poor application performance and outages can cost as much as £3 million an hour.⁶

However, financial costs look insignificant when compared with the negative impact on customer perceptions. Internet enabled businesses and consumers have rapidly become used to instant gratification and no longer accept service disruption, no matter how short.

In today's world hard won customer loyalty is threatened by any downtime.

³ http://www.nccmembership.co.uk/pooled/articles/BF_WEBART/view.asp?Q=BF_WEBART_286537

⁴ <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

⁵ http://news.bbc.co.uk/1/hi/uk_politics/7168588.stm

⁶ http://technology.timesonline.co.uk/tol/news/tech_and_web/article2277632.ece

The Full Cost Of Risk

A 2006 study by the Ponemon Institute, a privacy and information management research firm, found that the total cost of data security breach responses were up 30 per cent on the previous year. The investigated breaches cost the affected firms between US\$1 million and US\$22 million thanks to four related costs: legal and administrative expenses, lost business, managing customer inquiries, and, crucially, restoring a damaged reputation.⁷

It's no surprise that a firm's operational risk management processes have become a big influence on key economic performance indicators such as shareholder value and stock market ratings.

Executives, analysts and investors understand that well-targeted and effective measures are essential both to a firm's stability and growth potential.

Risk Ratings

Already, the quality of a firm's risk management influences financial ratings published by organisations like Moody's and Standard & Poor's. According to Moody's: "operational risk management improves the quality and stability of earnings, thereby enhancing the competitive position."⁸

Firms looking to take out loans or extend lines of credit will also have their practices evaluated by banks. Basel II regulations require checks to limit the amount of capital financial services institutions have locked into risk-related financial reserves.

Such concern is justified. A study of the time that large international companies can take to recover from incidents is sobering. While around half of companies were able to restore their stock market valuations within a year, 28 per cent took three or more years to do so, if they achieved it at all.⁹

But while it's easy to understand the importance of managing operational risk; it's not easy to do it within reasonable cost and time scales.

False Assessment

This is caused, in part, by the breadth and complexity of the task: almost every organisational action involves a degree of operational risk. The key is to assess and understand risk and test existing mitigation measures. The approach is far from straightforward, given the endemic tendency of organisations to view issues on departmental lines.

Nevertheless, improved risk management controls have improved in the face of the regulatory onslaught. A Compliance Week survey, conducted by the researcher, Audit Analytics, found that, over the three years since the introduction of Section 404 within SOX, the reported number of internal control failures reduced by almost 45 per cent.¹⁰ Yet evidence suggests responses can be inappropriately focused and disproportionate.

Inappropriate Responses

A firm's choice of risk management response has major cost implications. Approaching the task as a series of one off projects, rather than one ongoing activity, tends to require a bespoke project team to address each new threat. The teams often involve valuable employees who work under great executive pressure to conclude projects quickly and effectively.

The approach delivers major continuity problems:

- Removes key staff from core business activities;
- Creates regular projects vacuums as staff return to key job;
- Results in duplication, lost learning, inconsistent measurement and makeshift processes.

⁷ http://www.networked.bt.com/pdfs/Overcoming_applications_ignorance.pdf

⁸ http://www.ponemon.org/press/Ponemon_2006%20Data%20Breach%20Cost_FINAL.pdf

⁹ <http://www.gloriamundi.org/picsresources/maf.pdf>

¹⁰ http://www.deloitte.com/dtt/cda/doc/content/us_assur_Value%20Killers%20Report%20.pdf

The Death Of Innovation

Many firms are concerned that their response to new legislation has been too expensive and poorly aligned with long term interests.

Top executives, concerned by business and personal responsibilities, have demanded swift and decisive action. The obvious response to uncertainty is 'gold plating' mitigation measures to reduce risk exposure to an absolute minimum.

Aside from the obvious expense, the problem with this approach is that it doesn't necessarily deliver the right results. Enterprises need end-to-end business processes that deliver goods and services to customers but tend to simply join together discrete components with often limited effect.

Box Ticking

As Cynthia Glassman, Under Secretary for Economic Affairs at the US Department of Commerce, has noted, many firms have become risk-averse. Speaking in May 2007 about Section 404 of the Sarbanes-Oxley Act, she observed that "what was meant to be a top-down, risk-based management exercise had become a bottom-up, check-the-box auditor exercise" and that some of firms' efforts "are spent on activities that do not add much, if any, value."

The end result is a generation of businesses reluctant to take calculated risks on innovations that may secure their futures.¹¹ Ms Glassman also commented that "boards and management continue to spend more time on compliance and less on business strategy" than is good for their firms.

Her concern has since been corroborated by a survey conducted for NYSE Euronext by Opinion Research Corporation. It found that 78 per cent of CEOs were spending more time on regulatory and compliance issues than they had previously, and that 51 per cent were spending more time on risk management specifically.¹²

This has significant consequences. Kept busy elsewhere, comparatively few of the CEOs - only 32 per cent - found more time to spend on customer relationships. Perhaps even more worryingly a majority of CEOs felt the overall cost of managing risk and achieving compliance was a more important influence on their firms' future than new product development.

A Balanced Risk Approach

Many organisations know they are struggling to respond to the new risk landscape with a sensible level of investment in money, manpower and materiel. They don't want to gamble or halt progress.

Organisations need to re-evaluate their response to operational risk. The essential first step is a detailed review of business processes, supporting IT environments, key performance and risk controls, and mechanisms to identify and respond to emerging threats.

The suitability and cost-effectiveness of risk mitigation measures must be examined on an ongoing basis. The technology situation, for one, is in flux and the weapons used by hackers and fraudsters are evolving as rapidly as organisational defences.

Building Boardroom Awareness

One immediate organisational problem involves making operational risk reports available to boards and executives. Risk despatches are invariably hand-crafted, time intensive, poorly conceived and, out of date upon delivery.

Produced weekly or monthly, they tend to provide executives with a past, rather than a current, view on the threat landscape. Executives don't want to drill down and explore issues in depth but the production of bespoke reports is usually considered too expensive.

In today's dynamic world of business, such limitations are no longer acceptable. If top management want operational risk management to be more than the Ms Glassford's box-ticking exercise, they need accurate information that's refreshed in realtime and fit for the task at hand.

"Firms need to improve their internal information systems and communication mechanisms to ensure that senior management and boards of directors receive accurate, near realtime information on the causes, financial impact, and possible solutions of control problems."

Deloitte & Touche LLP, 2005¹³

¹¹ http://www.forbes.com/leadership/2007/11/28/sarbanes-oxley-survey-lead-govern-cx_mk_1128compliance.html

¹² https://www.esa.doc.gov/GlassmanSpeeches/Costs_Impeding_Innovation.pdf

¹³ Opinion Research Corporation, "NYSE CEO Report 2008", April 2007

Organisations Learn To Manage Risk

Getting access to up-to-the-minute data isn't the only challenge. Organisations must align their risk management measures with their commercial objectives and adapt quickly and flexibly to changing environments.

What's increasingly clear is operational risk management practices are not entirely transferable. Organisational approaches according to industry, legal and regulatory framework and, crucially, their appetite for risk.

Organisations have different attitudes to risk: some prefer safe options while others push things to the limit. The Italian homeware company, Alessi, is one example of a company prepared to take a risk. It differentiates itself by constantly pushing the limits of product design and accepts that it will come up with more failures than its competitors. Indeed, failed ideas take pride of place in the company's museum.¹⁴

There are, however, other notable aspects of Alessi's attitude to risk. Its response to changing market conditions, for one, runs contrary to received wisdom. At times of recession, the firm innovates around problems. "When the waves are not too high, we follow the waves," said managing director, Alberto Alessi, when interviewed by Fast Company magazine in 2001." But when the waves become more dangerous, you may need to find something new."¹⁵

Respond To Conditions

Other organisations will make different choices but, they too, will need to adapt their stance quickly and flexibly as circumstances change. For example, an established firm entering a new market may need to drop a traditionally cautious approach to win market share.

Firms must consider the impact of mergers or acquisitions on operational risk management. Steps to resolve conflicts and align approaches often involve considerable expense and the impact should be an essential part of any due diligence procedure.

Organisations must adjust their approach when new threats are identified. One technology example involves the suspension of network and systems access while new defence measures are installed. Another sees the airline industry introducing new, baggage scans and security checks. Both cases involve commercial risk because, while customers want security, they demand fast, easy access to their networks or airports.

Bottom Up Or Top Down Approaches?

Traditionally, firms have planned resilience measures from the 'bottom up'. In other words, they look to protect individual assets from theft, accidental data loss and hardware failure.

This approach has worked well in the past, but is now looking outdated as businesses globalise and increase dependence on complex technology infrastructures. Problems are even more likely where parts of a firm's infrastructure or value chain are outsourced, virtualised and produced in a partnership with multiple service providers.

Common Errors

Most firms have a business continuity plan to help them restore systems in the event of failure. Yet there is growing evidence that steps designed to resolve local problems often fail to address the 'knock-on' damage. It isn't unusual to find process efficiencies by tackling restorative tasks in a different order with coordination along the value chain.

Risk assessors often look at the immediate monetary consequences of an incident and overlook broader, enterprise-level considerations: assessment on the impact to customers, shareholders, employees, regulators, competitors and the brand is often conspicuous by its absence.

Establishing Control

Firms will need to take several steps to address these issues.

The starting point is an over-arching risk management strategy for the whole business rather than operate with a loose patchwork of plans from various organisational units. A holistic approach must be flexible and adaptable enough to accommodate outsourcing agreements and any inter-organisational splits in the service value chain.

Ideally, such a strategy should be based on industry best practice. The guidelines outlined in the British Standards Institution's publicly available specification, PAS-56 are designed to protect the firm in every respect; limiting the chance of damage to a firm's profitability, corporate reputation, competitive position, regulatory compliance and share price.

¹⁴ http://www.deloitte.com/dtt/cda/doc/content/us_assur_Value%20Killers%20Report%20.pdf

¹⁵ <http://www.fastcompany.com/magazine/51/alessi.html>

Plan, Do, Check, Act

One option is for firms to base their risk management strategy on the renowned Deming 'Plan-Do-Check-Act' Cycle. The model is the basis of quality and performance management systems including ISO9000, ISO17799 and SixSigma.

The approach is easily customised to manage risk, taking into account the requirements and recommendations of advisory and regulatory bodies such as the Committee of Sponsoring Organisations of the Treadway Commission (COSO)¹⁶ and the US National Research Council's Committee on Risk Assessment Methodology (CRAM).

The result is a risk treatment cycle that gives equal weight to the identification and assessment of risks, the selection and deployment of controls, and the monitoring of their effectiveness – all while allocating proper and binding ownership for the risk management process.

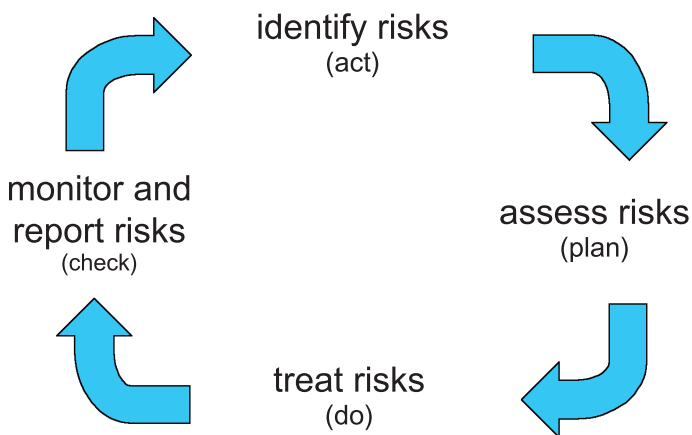


Figure 1: Deming 'Plan-Do-Check-Act Cycle

- **Step One: ACT** – Identify organisational risks and assign owners. Every type of risk must be explored, including legal and regulatory, human and physical assets, and the operating environment.
- **Step Two: PLAN** – Assess the significance of each risk. The tools include business impact assessments, past incident reviews and analysis of vulnerability assessments conducted for information security purposes.
- **Step Three: DO** – Categorise risks in four ways against likelihood and impact. Firms can avoid risks entirely, reduce risks, outsource risks or accept risks. A way of reducing risks, for example, would be to set intruder detection systems to limit unauthorised access.
- **Step Four: CHECK** – Monitor the performance of measures, record incidents and outcomes, and track changes in business or risk landscape. The information feeds back into step one to complete a virtuous circle.

A firm's risk management strategies must focus on protecting key stakeholder assets rather than the internal organisational structure or system and process design. Managers must prioritise the response to threats that would be unworkable in a bottom up matrix with specialists working in silos.

The approach does not spell the end for functional responses. The protection of key assets and critical infrastructure, such as data centres, does not end. It is, however, important to recognise their role as elements of a bigger picture.

Strategic Testing

Firms must test their risk assessment strategies. Assumption is, after all, the root of many disasters. A recent CSO Magazine survey, for example, found that, although 93 per cent had a business continuity plan in place, only 37 per cent of US companies had tested it.¹⁷

Unfortunately, such blind faith can give a dangerous false sense of security. One major British firm's business continuity plan was reputed to depend on moving 3,000 people from London's Docklands to the north of the city in 30 minutes – a journey of 17 kilometres through the heart one of the world's busiest cities. Apparently the CEO approved plan didn't include a rehearsal that would have demonstrated the flaws in the plan.¹⁸

In this case embarrassment was the only negative outcome, but the consequences for poorly conceived business continuity and recovery plans can be far more severe.

Firms must test plans at conception and at regular intervals to ensure staff can follow the procedures. All weaknesses from such rehearsals, actual incidents or near misses must be identified and reported back to inform plan updates.

¹⁶ http://www.deloitte.com/dtt/cda/doc/content/us_assur_Value%20Killers%20Report%20.pdf

¹⁷ <http://www.coso.org/>

¹⁸ <http://www.csoonline.com/csoresearch/report85.html>

Responding In Realtime

Firms must be able to respond rapidly to new threats designed to take advantage of weak points in global networks. The key to fast and direct response is an accurate, realtime, executive view that is aligned to risk information sources across the organisation.

“The dynamism of business results in rapid changes to business processes, relationships and technologies that firms must continually map to risk and compliance requirements”

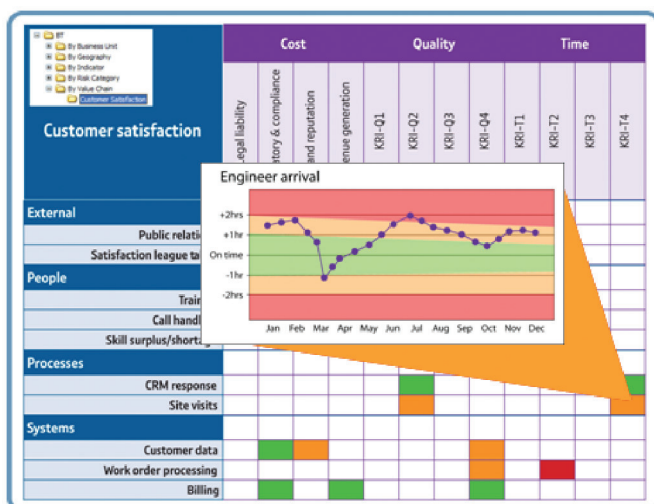
Forrester¹⁹

Many technology systems offer functionality but, in general, present information gathered from organisational structures and key assets in a raw form unsuitable for senior executives. Managers care about the impact on key business processes and how that affects customer satisfaction rather than the specific details in the detail of specific threats and controls.

Risk Reporting

An effective system collates information on risks to business processes and presents it to executives through simple, clearly designed interfaces. The information allows managers to identify and respond to any abnormal indicators that threaten business strategy.

Different views reflect different users from the CEO to compliance officers and make it easier for staff to understand the full spectrum of risks – including business continuity, security, compliance and operational integrity – and the effectiveness of the measures in place to mitigate them.



BT Risk Cockpit

Document, Retain And Reproduce

Every business needs to document and retain information for regulators and stakeholders.

Auditors and investigators can demand recent data and recorded data, going back several years, so both live databases and historical archives must be fully protected against misuse, alteration and deletion. Importantly, firms must ensure that archived records are accessible even when relevant technical platforms have been updated or replaced.

Success demands behind the scenes activities. Information must be gathered from a range of organisational 'sensors' like business processes, IT systems and knowledgeable individuals. The data must be distilled to create a set of risk and performance indicators directly relevant to the organisation's goals to allow for near time escalation. Similarly, mechanisms must feed back commands from executives to the field and ensure effective monitoring and documentation.

Behind the scenes engineering – in a way similar to an aircraft cockpit – delivers most key risk functions. The way sensors and controls are wired together makes a huge difference to the intelligibility and usefulness of displayed information and, consequently, a manager's ability to act decisively.

Deciding how to combine gathered information into give a flight deck overview requires expertise and experience that spans security, network, vulnerability and applications management.

The effort pays dividends. A firm with well configured risk management systems will provide all risk managers with guidance centred on a common view of a risk position matched to their personal role. Management control is improved. Risks identified, recorded and assessed. Risk mitigation plans created and tested with the results made available to management. All relevant activities are recorded, and retained for future evaluation.

The selected controls assure performance, effectiveness and compliance. Data about actual incidents and near misses are used as a further source of input to and feedback on risk management plans. Ultimately everything is related back to commercial and regulatory targets and which ensures investment in mitigation and compliance is appropriately targeted.

“Other than political lobbying, the only effective way to reduce the complexity and cost of compliance is through the application of IT that improves the compliance process and automates the instantiation and monitoring of controls.”

Gartner²⁰

¹⁹ http://www.deloitte.com/dtt/cda/doc/content/us_assur_Value%20Killers%20Report%20.pdf

²⁰ “Overcoming Risk and Compliance Myopia”, Forrester, August 2006

Gaining Advantage

The combination of the right risk management strategy and effective management systems will make it much easier for organisations to understand and control operational risks to their technology infrastructure. The data enables firms to manage laws and regulations and their own risk appetite.

But in a growing number of industries – especially the heavily regulated – firms need to go further to embrace the growing role of suppliers and partners in their risk management approach.

Pharmaceutical Industry – Extended Value Chains

The pharmaceutical industry is home to some of the world's biggest and fastest-growing businesses, but it faces major challenges. Regulators demand stringent standards across an already stretched development, testing and approval cycle. Issues like detailed record keeping make it tougher and more expensive to bring new drugs to market.

US Food and Drug Administration (FDA) standards are among the world's most stringent and significant: 40 per cent of all drugs are sold in the US. Every step in the drug development process must be documented in detail and companies have to demonstrate information credibility as people pass details across networks and computer systems. Failure to meet these exacting standards results in severe penalties. The FDA has power to shut down manufacturing plants down and levy fines up to US\$500 million before a company faces criminal or civil prosecution. Naturally such action hits profits and share prices.

Increasingly, however, key knowledge and mitigation processes sit with expert outsourced suppliers. Choosing suppliers that document and operate products in line with industry regulations provides firms with significant advantage through access to ready made systems.

BT Experience

Increasingly, service providers will need to become part of their clients' mission-critical infrastructure and value chain. For example, BT's Pharmaceutical Compliance Office oversees the delivery of the company's services to clients in the sector. It makes sure products and services are operated in ways that align with FDA, EMEA and other pharmaceutical industry regulations and inherently deliver the documentation clients require, making their lives that little bit easier.

Gaining Insight

Firms that outsource the provision and support of their networks and IT systems are likely to need support from their suppliers when considering acquisitions or starting new relationships. Interconnecting infrastructures and rationalising solutions inevitably creates risk that requires rapid analysis and mitigation plans.

Such expertise, in a complex world, generally lies with the supplier. Firms must consider whether suppliers have an adequate understanding of the unique circumstances.

Questions revolve around whether theoretical understanding transfers into solid practical experience of what's required. Has the supplier undertaken similar deals itself, for example? And have these been of relevant scale and scope? Such factors matter a great deal when it comes to assessing the risks a firm might be taking on, undertaking due diligence exercises and so on.

BT Experience

In a knowledge-based business, one of the biggest threats to success is that key personnel affected by a deal will become unsettled and. Alert to the possibility, BT has put in place a range of procedures designed to maintain the motivation and commitment of those involved in its acquisitions, the net effect of which has been that only one key person has been lost over more than two dozen deals.

BT is also a keen adopter of outsourcing, and is similarly concerned that the expertise it 'loses' to the selected suppliers continues to be available to add value to its business. Under contracts valued at more than £500 million per annum, more than 7,000 of our people have been transferred to other companies. The contracts cover software development, computer support, the operation of contact centres, facilities management, and HR, accounting and financial services.

Conclusions

Despite the growing emphasis on operational risk management many firms cannot claim even an appropriate level of control, especially when their business processes and service models are adapting to new challenges. At such times organisations often face large risk exposure.

Regulatory timescales are tight and the consequences of failure are severe. Unsurprisingly, many firms have gone for simple, 'gold plated' solutions to avoid putting their managers and themselves in court. The result, however, is that organisations have become risk averse – reluctant to innovate and secure their future.

To complicate the situation the business landscape is changing faster than ever before. New technology has enabled radical new ways of working, new ways of doing business with customers and the globalisation of operations and supply chains, transforming performance and efficiency.

Risk to Reward

But these advances have come at a cost. Open, extended networks and high-performance IT systems deliver new possibilities and new risks. The promise of bottom line impact can be lost with ineffective risk management.

Mastering risk management and controls that can respond in realtime to new threats means protecting new prospects and profits. Negligent risk management means opening the door to new threats and losses. The challenge is immense and, to meet it, firms must deploy methodology and tools:

- Review risk management strategies;
- Focus on end-to-end performance rather than protect operations and assets;
- Bring in IT systems that provide realtime views of risks to enable realtime response;
- Demand suppliers reduce risk management costs associated customers.

As technology based value chains become extended, more open and virtualised, firms will need expert insight to cope with risk and complexity as they strive to improve business processes and manage change. Suppliers must earn the trust of the organisations they serve.

But perhaps the most important element of operational risk management is to remember why regulators focussed on it in the first place. Too many organisations were gambling. As the army General, George Smith Patton Jr, once advised: "Take calculated risks. This is quite different from being rash."

Outsourcing risk – how to choose your partner

1. **Ask around.** Find out what analysts and others have to say, both for and against.
2. **Check for substance.** Does the supplier have enough people with the right qualifications and the financial and other resources it will need to discharge its responsibilities?
3. **Value experience.** 'Bright young things' have their value, but in a difficult situation, it will often be the people who've 'been there and done that' that you'll depend on.
4. **Look for value-add.** Suppliers with customers in several different sectors will be able to take learning from one and apply it to the advantage of others. You stand to benefit.
5. **Go for breadth.** Business doesn't stand still, so it might not be in your longer-term interest to choose a supplier with a limited service portfolio.
6. **Make a match.** Pick a supplier that can manage risk in a way that's right for you. If it can provide document its services in the format you need, you'll have much less work to do.
7. **Choose a peer.** If you are large and global, pick a supplier that is as well. It's more likely to understand the challenges you face and be able to address them.
8. **Buy into a vision.** No one knows exactly what the future holds, but some have a better idea.

1. Jericho Forum Mission Statement - <http://www.opengroup.org/jericho/>
2. "Risk and reward - getting the right balance", ITadviser, Issue 48, March/April 2007, http://www.nccmembership.co.uk/pooled/articles/BF_WEBART/view.asp?Q=BF_WEBART_286537
3. "Risk and reward - getting the right balance", ITadviser, Issue 48, March/April 2007, http://www.nccmembership.co.uk/pooled/articles/BF_WEBART/view.asp?Q=BF_WEBART_286537
4. Privacy Rights Clearinghouse, "Chronology of Data Breaches", <http://www.privacyrights.org/ar/ChronDataBreaches.htm>
5. BBC News, "Tougher Data Laws Needed, say MPs", January 3, 2008, http://news.bbc.co.uk/1/hi/uk_politics/7168588.stm
6. "Skype Outage Hits 220 million Users", Times Online, August 17, 2007, http://technology.timesonline.co.uk/tol/news/tech_and_web/article2277632.ece
7. Yankee Group, "Overcoming Applications Ignorance: New Services to Enable Agility", April 2006, http://www.networked.bt.com/pdfs/Overcoming_applications_ignorance.pdf
8. "Ponemon Report Shows Sharp Rise in the Cost of Data Breaches", Ponemon Institute, October 2006, http://www.ponemon.org/press/Ponemon_2006%20Data%20Breaches%20FINAL.pdf
9. "Moody's Analytical Framework for Operational Risk Management of Banks", Moody's Investment Services Corp, 2003, <http://www.gloriamundi.org/picsresources/maf.pdf>
10. "Disarming the Value Killers", Deloitte & Touche LLP, 2005, http://www.deloitte.com/dtt/cda/doc/content/us_assur_Value%20Killers%20Report%20.pdf
11. "Huge Progress in 404 Compliance", Compliance Week, November 2007. Reported in Forbes at http://www.forbes.com/leadership/2007/11/28/sarbanes-oxley-survey-lead-govern-cx_mk_1128compliance.html
12. Cynthia Glassman, "Are Regulatory Costs Impeding Innovation?", Speech to the American Enterprise Institute, May 2007, https://www.esa.doc.gov/GlassmanSpeeches/Costs_Impeding_Innovation.pdf
13. Opinion Research Corporation, "NYSE CEO Report 2008", April 2007
14. "Disarming the Value Killers", Deloitte & Touche LLP, 2005, http://www.deloitte.com/dtt/cda/doc/content/us_assur_Value%20Killers%20Report%20.pdf
15. "Failure is Glorious", Fast Company, September 2001, <http://www.fastcompany.com/magazine/51/alessi.html>
16. "Disarming the Value Killers", Deloitte & Touche LLP, 2005, http://www.deloitte.com/dtt/cda/doc/content/us_assur_Value%20Killers%20Report%20.pdf
17. The Committee of Sponsoring Organisations of the Treadway Commission, <http://www.coso.org/>
18. "Business Continuity Survey", CSO Magazine, January 2005, <http://www.csoonline.com/csoresearch/report85.html>
19. "Disarming the Value Killers", Deloitte & Touche LLP, 2005, http://www.deloitte.com/dtt/cda/doc/content/us_assur_Value%20Killers%20Report%20.pdf
20. "Overcoming Risk and Compliance Myopia", Forrester, August 2006
21. "Survey on Sarbanes-Oxley Compliance Practices Within IT Organizations and Businesses", Gartner, September 2006

Offices worldwide

The 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 respective standard conditions of contract. Nothing in this publication forms any part of any contract.

©British Telecommunications plc 2008.
Registered office: 81 Newgate Street, London EC1A 7AJ
Registered in England No: 1800000

PHME 55053

