

Managing Operational Risk for Performance and Competitive Advantage

A White Paper from BT

Contents

Introduction.....	3
Executive Summary	3
Operational Risk is Central to the Organisation	4
The Aftermath of Compliance –a Birthplace for ORM	4
Visualisation of Risk –dashboard vs cockpit	5
Learning from the Past –Anticipating the Future	6
Bringing it all together - the Full ORM Framework around the Cockpit Hub	6
The Emerging Risk Agile Organisation	7
The Emerging Risk Agile Supplier.....	7
Where to Begin?.....	7

Introduction

Stringent corporate governance, regulatory standards and investor expectations increasingly make risk management a focus for all large organisations. The challenge is not just about avoiding risk or simply reacting to new regulation. It is about operating within a targeted level of operational risk whilst complying with regulatory and corporate guidelines. It is also about aligning these with business objectives and using the risk and control information to maximise operational performance, minimising cost and achieving competitive advantage.

This white paper will propose and summarise an overall framework of capabilities, disciplines and technologies built around the hub of a “Risk Cockpit” for Operational Risk Management in the networked IT space. It will describe the nature of the new organisation that will emerge from the embracing of operational risk management for performance through a Risk Cockpit.

Finally, it will suggest how the considerable investments made thus far for compliance will yield returns to the enterprise and its stakeholders and fundamentally change their relationship with their suppliers.

Executive Summary

The role of Risk Management in reducing volatility, increasing stability and predictability, and promoting transparency in organisations’ operations has become enshrined in the majority of recent corporate governance and regulatory standards. Risk management now touches enterprises beyond those whose business is traditionally based on risk and have highly developed tools and techniques (e.g. the financial sector).

Risk Management must not just be about avoiding the bad things – staying out of prison, staying out of court, staying out of the papers – but on how you want things to be in your organisation. If you want success you must plan for success, you must set up your organisation so that it can arrive at its destination reliably and safely.

This clearly dictates a proper understanding of risk in the organisation, but also how these risks might threaten the corporate objectives and strategy. This paper describes how such a starting point is a key enabler to driving operational risk management for performance and competitive advantage.

The proper understanding, assessment, measurement and monitoring of risk affords a detailed insight into the internal and external environment in which the enterprise operates and how it operates. Such insight should be a key enabler for better corporate decision-making.

The paper discusses risk from an Enterprise Risk Management (ERM) perspective.

In the Digital Networked Economy, enterprises compete and survive on their information. The establishment of a reliable and assured networked IT infrastructure is vital. For the modern organisation, networked IT risk poses the largest common threat to operations and the biggest opportunity for mitigation.

A key component of enablement is placing the right information in the right context in front of the user, but we argue that this visualisation of Operational Risk Management must go beyond dashboards, and cannot remain as a science of reporting and assessment.

Our paper will propose and describe an overall framework of capabilities, disciplines and technologies built around the hub of a Risk Cockpit for Operational Risk Management and illustrate its usage in the networked IT area of risk. The Risk Cockpit, as its name suggests, must provide the dashboard required by the user but should also provide the control and safety features needed to drive operational risk for performance.

We recommend organisations adopt an ERM strategy that encompasses Operational Risk thus ensuring a consistent and coherent risk strategy.

This paper will also describe the nature of the new organisation that will emerge from the embracing of operational risk management for performance through a Risk Cockpit. It will suggest how the considerable investments made thus far for compliance will yield returns to the enterprise and its stakeholders and fundamentally change their relationship with their suppliers.

Operational Risk is Central to the Organisation

"... the investment community may well adopt operational risk as one of the fundamental metrics it uses in the evaluation and valuation of companies in virtually any industry. Operational Risk may well take its place alongside such benchmarks as p/e ratios and turnover..."

Dan Geer - "Basel II - Being Security Conscious"
ITsecurity.com

When looking at Operational Risk many start by examining the Basel II definition:

- The risk of direct or indirect losses due to failures in systems, processes, people and external factors. This includes legal risk but excludes reputational and strategic risk.

More generally, Risk Management is defined as:

- A process by which risk is identified, measured (quantitatively and/or qualitatively), mitigated and monitored on a regular basis.

Both definitions focus on the mitigation of risk, i.e. the limitation or avoidance of loss through proper understanding of risk exposure and the mitigating effect of applied controls.

There is no doubt that this level of understanding is vital in surviving adverse situations, but business is not just about avoiding risk. It is also about risk appetite and response. It is about knowing when to take a risk and knowing what risks to take.

The AS/NZ 4360:1999 risk management standard offers what we believe is a highly mature definition of risk and risk management:

Risk: "The chance of something happening that will have an impact on objectives."

Risk Management: "The culture, processes, and structures that are directed toward realizing potential opportunities whilst managing adverse effects."

If organisations highlight the adverse and ignore the opportunity, the systems and processes they deploy will be more likely those that can accurately portray the situation. You can liken this to a war correspondent that

can tell you what the war is like at the front line but cannot change the situation.

Investing in risk mitigation to achieve the stability sought by stakeholders (investors, etc.) is laudable but is that the totality of its justification? This paper contends that Operational Risk should also be driven for performance. In order to make this a reality in an organisation a suite of supporting processes, tools and services are required so that the organisation can:

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

The Aftermath of Compliance – a Birthplace for ORM

In the aftermath of the compliance efforts of recent years it is vital to set about effective risk management and leverage the greater levels of understanding of operations gained through that process.

Regulatory and Compliance Reporting

Regulatory compliance reporting and the associated support for internal and external audit functions is an ongoing cost that cannot be avoided. It is therefore an infrastructure cost for the organisation that allows it to continue to operate and must be made as cost efficient as possible.

Recent studies show that up to 40% of a company's IT budget can be spent on compliance, in other words paying to stand still. Boards must address the requirement to create more shareholder value and translate this cost into an investment.

The frameworks of regulation can be dissected into mandates that further map to controls within the organisation.

Risk and Control Assessments

The problem with the resulting pure compliance reporting is that the controls are assessed as individual points. This limits their value and yields little return on their cost as it prevents two key abilities:

- The ability to do a single audit in a business unit encompassing multiple themes with a resulting single mitigation strategy;
- The ability to re-slice to look at a compliance view to validate such strategies across business units.

Exposure Calculations

Controls need to be viewed alongside the risks and threats in the organisation that these controls are mitigating. Their effect on the risks they mitigate must be captured and the risk itself assessed so that the residual risk can be calculated.

A single assessment of the above has limited value as it can only show the situation now. For the risk to be managed all these measures need to be gathered on a regular basis as appropriate to the risk's nature.

KRI/KPI Repository

The effective management of risk requires a regular feed of key risk and key performance indicators (KRIs, KPIs). These must be combined with the regular human audit and assessment to establish an effective set of processes and procedures for the management of controls and risks.

The risk appetite for the organisation and the performance targets for the controls can be expressed using thresholds; thresholds for Green (acceptable), Amber (cautionary) and Red (unacceptable) must be set to trigger management attention.

Risk Register Reporting

Most organisations manage their risks through risk registers and indeed evidence of this style of management is encouraged by much corporate governance guidance. Having gone to the trouble of gathering a hierarchical repository of risks and controls it is vital to express it to the risk managers in terms of their risk registers. The Risk Cockpit will make this register alive and active – a Living Risk Register.

Loss History and Near Misses

The final piece to this core is the light of experience of when risks become, or get close to becoming, real events (loss events and near misses). It is vital to capture these, as this is your only evidence of the behaviour of the risk as it costs and impacts your organisation.

Risk Cockpit

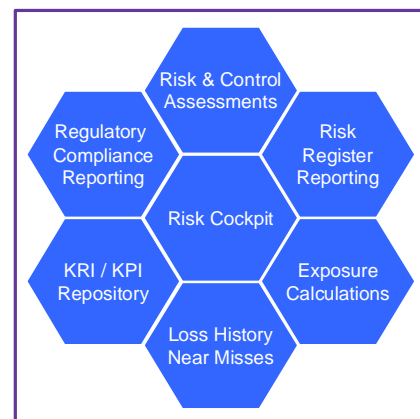
It does not take much to realise that the management of the relationships between the hierarchies of risks and controls cannot be sustained using a federation of documents and spreadsheets. The overhead and opportunity for inaccuracy (and hence rendering worthless the effort) is too high.

In our experience, all organisations reach this precipitous point where there are two choices:

Allow technology and constrained process to be the limiting factor accepting that risk management will never penetrate the depths of the organisation nor be consistently applied across its breadth.

Make a suitable investment in a supporting toolset to allow risk management to accelerate and evolve, limited only by culture and an understanding of the risks and controls themselves.

The tool needs to support the framework of components discussed so far with equal strengths in its abilities to regularise assessment, measurement, reporting and management process:



This is the essence of the Risk Cockpit and at this point it is worth explaining why we deliberately use the term "cockpit".

Visualisation of Risk – dashboard vs cockpit

Corporate dashboards are very much in vogue at present and provide users with consolidated views of aspects of their organisation – i.e. dimensions of importance. A dashboard, as its name suggests, is connected to what lies under the bonnet (to use a car analogy) and provides the right level of summary information for the driver to operate the vehicle and arrive at their destination in safety.

Risk management needs more than the information "under the bonnet". Risk management is a human activity about risk appetite and response but also about knowing when to take a risk and what risks to take. For that reason it must be able to take input and direction from the driver – this is what makes it a cockpit.

BT's accompanying whitepaper "Creating and Sustaining Risk Agility and Compliance with the Risk Cockpit" describes in more detail what the core of the Risk Cockpit must provide in terms of navigation and visualization. Ultimately, the Risk Cockpit becomes the hub of the organisations risk management and provides all the information needed to properly maintain the assessment, monitoring and management of risk.

Many organisations fall short of achieving this, and it is rarely because the information is not available. Rather, it is usually due to the limitation of the federated documents and spreadsheet solution currently in place.

We contend that such infrastructure cannot sustain the level of risk management and compliance now required for modern business and as such, the Risk Cockpit is more than a function it is an application in its own right.

Learning from the Past – Anticipating the Future

In its basic form risk management can operate at a level to limit the effect of adverse conditions i.e. the risk information used to detect emerging situations such that the appropriate management actions are put in place to regain control or to limit loss and impact.

Risk Management Lifecycle

Risk management however needs to be part of a formalised and supported continuous improvement programme (a risk management lifecycle) involving regular audit and assessment, the ability to analyse from experience to determine improvement and the ability to manage action plans for those improvements and measure their success.

Business Case

The data on the risk exposures and effect of control can be used to build the business cases for the investment programmes ensuring that budget is spent wisely, only where it is needed and only to the extent that it brings the risk within the desired appetite for the organisation.

Change Management

The action plan can be utilised to co-ordinate the change management required to prosecute these risk improvement strategies and indeed the risks associated with the change programmes can be captured and monitored in the cockpit.

Benchmarking

The historical repository can be used in internal benchmarking of risks and controls to ensure consistent performance across the organisation e.g. CRM centres. Key indicators may also be used with peers in the organisation's industry to establish benchmarking for the organisation externally.

At Risk Process Engineering

The risk model and history will help to highlight the elements in the organisation's operation that pose the most serious exposures. Modern organisations have to be capable of change and re- structuring to remain agile and competitive. Organisations are therefore increasingly process based rather than structure based regarding their operations and as such analysis of the operational risks in

these processes is vital if they are to be engineered to sustain an acceptable level of risk.

Horizon Scanning

Looking to the future the organisation needs to make sense of its environment and how it might change over time. Utilising a combination of past history, the establishment of external indicators (to sense the environment) and the ability to conduct what-if and scenario modelling the horizon can be scanned and informed strategy decisions made. Once again this is part of the Risk Cockpit's role and distinguishes it from a "dashboard" whose view is fixed looking backwards like a 'rear-view mirror'.

Not only is the cockpit forward looking, it is beginning to provide expert opinion, and being used to set up sensors and analysis that will determine which way the environment will change and hence what the organisation may wish to do in anticipation of this.

Bringing it all together - the Full ORM Framework around the Cockpit Hub

So far we have described the rich combination of components required to establish the capabilities demanded of a Risk Cockpit.

Data Quality Management

The cockpit runs on the availability of good quality data from the operational environment and conscious action must be taken to maintain and safeguard those quality standards and prevent bad data polluting the cockpit and its displays.

Furthermore the cockpit as the hub for risk and compliance holds a history of risk and control performance and assessment data in support of the risk and control management process.

Information Management (assurance)

For many compliance regimes information related to policies and controls must be managed under a strict process of definition, maintenance, communication/publication, acknowledgement and training. All the supporting evidence of the process, its instantiation and success must also be available to the auditor.

For auditors to be happy to use this information in their attestations of the effectiveness of controls or for the information to be deemed acceptable as evidence of operation, it must be both assured and managed throughout its lifecycle and in compliance with corporate policy. Without this, the information loses its provenance.

Risk Treatment

Risk treatments represent the larger proportion of an organisation's investment in the management of operational risk. In any other field of business, an investment decision is only made based on sound knowledge and yet often in the realm of risk there can be a desire to mitigate the risk whatever it takes. This is neither sustainable nor sensible but without the framework of components built around the Risk Cockpit it may be the best an organisation can do.



The Emerging Risk Agile Organisation

The ORM framework built around the hub of a Risk Cockpit will enable the transformation of risk management in organisations from a fragmented, subjective, inconsistent application of techniques, judgement and reporting to an action orientated and aggregated view across the business utilising real data, consistent aggregation, clear ownership, aligned action plans and trend information.

This creates new possibilities for building the true "risk agile" organisation characterised by a strong risk management mindset and culture across the enterprise.

The Emerging Risk Agile Supplier

The levels of complexity and corresponding levels of skills and investment needed to sustain the right levels of control against risk and compliance mean that for many aspects of networked IT this has gone beyond the core competence of the organisation's own IT department. In any event, this is often not the core business of the organisation.

The best way to gain and sustain the expertise is to go to a supplier organisation whose business it is to provide this networked IT, and who can deliver the services in such a way that reliably deals with the operational and enterprise risk.

This is certainly critical for the emerging risk agile organisation described in the previous section.

The supplier should show they use these techniques as part of managing their own operations and have the appropriate evidence and accreditations to prove it.

The age of the commodity supplier is ending and the age of the risk aware and agile supplier is dawning.

Where to Begin?

Modern organisations are reliant on their networked IT services to operate. It is on these that an organisation's people and processes rely. It is here then that proper risk and control needs to be applied with the expertise of risk agile suppliers of networked IT services.

The journey to achieving the levels of risk understanding and management proposed by this paper cannot be achieved overnight. The best way to implement the programme is to break it down into manageable, benefits driven investments aligned to the corporate goals of the organisation.

As the nature of risk is to change over time we recommend implementation of risk, compliance or control areas should be scoped and time boxed into 90 day implementation cycles based on a 10-20 day capture, analysis and prototyping phase.

This ensures focus is achieved from the outset, exemplars can be implemented quickly as a catalyst for change, and an unwavering quest for benefits realisation i.e. driving risk for performance and competitive advantage, is established to sustain the programme.

Steve Benton, Senior ORM Consultant, BT Global Services.

About the Author

Steve Benton is a senior ORM consultant in BT's Business Continuity, Security and Governance Practice. He has over 10 years experience, working with global clients, advising on operational risk management strategy and services.

For more information about BT's
Operational Risk Management Service
and the BT Risk Cockpit visit
www.bt.com/globalservices
or contact your BT account manager

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 2006
Registered office: 81 Newgate Street, London. EC1A 7AJ
Registered in England No. 1800000.

All Rights Reserved. Reproduction and distribution of this publication in part or whole, in any form, without prior written permission is forbidden.

