Operational Risk Management and IT: 
Implications for Financial Services
Introduction

Operational risk is moving up the boardroom agenda within financial institutions, driven by well-publicised threats to business operations and a rising tide of regulation. With robust mechanisms in place to manage market and credit risk, firms are increasingly considering an integrated approach that also encompasses operational risk.

Executives within financial institutions recognise the need to invest, but are concerned that the cost and complexity of addressing IT risk outweigh the benefits. As a crucial enabler of the modern financial services sector, IT permeates the entire organisation, making it a major contributor to the risk profile.

This paper examines the impact of IT on operational risk, describes how some financial institutions are realising substantial benefits by making the right investments and considers some of the options available.
A significant management challenge

High profile threats such as terrorism, fraud, natural disasters and well-publicised technology failures, along with the associated increase in the volume and complexity of regulation have highlighted the importance of operational risk management for the financial services sector. As a result, boardroom executives are demonstrating an increased desire to understand, control and minimise such risk. Indeed in some financial institutions, they are already being measured personally on the effectiveness of their processes in meeting a wealth of regulatory pressures. Datamonitor has recently published a report that covers more thoroughly some of the legal and regulatory controls currently impacting financial institutions.

Work carried out by the Basel Committee as well as researchers and risk managers at major banks is shaping emerging operational risk management practices. The Basel Committee defines operational risk as: the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Many organisations would extend this definition to cover events that can substantially erode an organisation’s value — by damaging its reputation for example.

In some financial institutions, boardroom executives are being measured personally on the effectiveness of their processes in meeting regulatory pressures.

Many financial institutions are beginning to include operational risk in the mix of overall risk so that it can be integrated into the economic allocation of capital across business units. By achieving this, they introduce a “risk cost” to individual parts of the business that acts as a driver for risk reduction throughout the organisation.

Even with this increasing effort, however, managing operational risk remains a challenging task. The fact that the risks involved span the entire organisation from end-to-end adds complexity and operational risk reduction is perceived as a high cost activity.
As firms struggle with the control of operational risk, financial industry regulators are increasing their efforts in the same area. They are developing an interlocking framework of requirements that focuses on the active assessment and management of all operational risks and, as the burden of regulatory measures imposed on the financial services industry continues to grow, managing risk and compliance has become a major area of spend in most financial institutions.

It is becoming clear that much of the emerging legislation has common process, reporting and data gathering requirements. This supports the hypothesis that integrated, enterprise-wide solutions may be the most efficient and effective approach to compliance.
IT risk pervades operational risk

Many financial institutions are still not satisfactorily addressing the significant operational risk posed by the technology on which their businesses rely. IT has become the critical backbone supporting a sector that operates in global markets, with complex products, huge data volumes, complex IT environments that have resulted from mergers and acquisitions, and a history of bolting the latest functionality onto existing systems. While many senior managers undoubtedly recognise IT as a risk to their businesses, a significant number are still overlooking the full extent or potential impact of the risk.

As the critical backbone supporting the financial services sector, IT is not only a direct risk, it is also a risk multiplier.

An Economist Intelligence Unit survey\(^2\) shows that nearly half of the senior managers surveyed consider digital risk as a high or very high risk to their businesses and 60% said they had suffered financial loss as a result of system outages in the previous 12 months.

This research, along with an Economist Intelligence Unit paper on the role of the CRO\(^3\) gives a good insight into current thinking on the role of IT in risk.

There are plenty of examples of financial institutions suffering severe direct impact when weaknesses have occurred around controls and IT.

- Up to 45% of the market capitalisation of a company was lost overnight when a control weakness came to light
- Another financial institution has been barred from any major new acquisitions until it solves its compliance problems
- Computer hackers broke into data banks at an American credit card processing facility, exposing the account numbers of more than 40 million cardholders
- More than half of a large US bank’s ATMs went offline for a weekend due to a computer virus, severely impacting the reputation of the bank.
Technology is more than just a direct risk, however, it is also a risk multiplier. IT systems are used to monitor, measure and manage the institution’s entire risk profile and demonstrate regulatory compliance, for example, so IT failure can have significant risk management consequences. In client studies IBM has assessed the impact of IT risk in business disruption and system failure upon other areas of operational risk. The findings show quite extensive impact.

The problems posed by IT risk are not unique to the financial services sector. In a recent cross industry survey conducted by the Economist Intelligence Unit (EIU)^4, of the fifteen categories of risk assessed, the top three risks identified as a threat to global business operation related to human capital (for example staff shortages and succession), risks to reputation, and IT risk (such as loss of data and outages), confirming that IT is high on the risk agenda. The fourth most significant threat identified was regulatory risk.

Figure 2: An assessment of the risk categories impacted by IT – from client studies (source IBM)
Managing IT risk to realise business value

There are direct business benefits to be gained by those who invest in IT for risk management. Using innovative tools and methodologies, IBM can help institutions to evaluate their risk profile and focus action on those risks that prove to be most significant. Recently, IBM was able to show one global banking group that, by improving focus on specific areas, it could reduce system downtime by 25% and save around $24 million per year in one part of the group alone. In another, the benefits of outsourcing resulted in a reduction of over $120 million per year in the total amount of regulatory capital that the group had to set aside against risk.

Investment in an improved risk profile can also drive specific new business opportunities for financial institutions. The case study based on a leading settlement house illustrates how the company worked with IBM to design, develop and manage the IT applications and infrastructure that support its uniquely secure foreign exchange process. The resulting reduction in risk has led to Forex dealers operating with improved credit limits and large corporate organisations recommending that their investment managers use this settlement house in order to reduce their own risks.

Implementing effective IT solutions can significantly reduce the costs of regulatory compliance. Regulators expect financial institutions to have resilient IT systems, but institutions also use their IT systems to demonstrate that they are meeting other aspects of regulation, for example by logging activities that can then be audited to prove compliance. Reliable, enterprise-wide systems can dramatically cut the associated costs and risks.

Investment in robust IT that supports business resilience may also provide further return in the form of lower insurance premiums. Companies that can demonstrate genuine business resilience with the correct controls in place will find insurance companies prepared to deliver favourable terms, a fact confirmed by Stokes and Platten.  

There are direct business benefits to be gained by those who invest in IT for risk management.
Leading settlement house transforms worldwide foreign exchange trading with help from IBM

The challenge
To eliminate the risk of default on foreign exchange dealings caused by time zone differences between global banks. Foreign exchange settlement processes needed transforming to enable the simultaneous and real-time settlement of payment instructions associated with foreign exchange transactions.

The solution
To design an innovative, real-time process for the settlement of payment instructions associated with foreign exchange transactions. To partner with IBM to design, develop and manage the IT applications and infrastructure needed to support the uniquely secure new process. IBM now runs the applications and infrastructure as a service to the settlement house.

Business benefits
The system:
- Is now the preferred way of settling global FX payments, handling volumes which peak at over 500,000 transactions a day and involving total daily currency trades sometimes in excess of $5 trillion
- Eliminates the foreign exchange settlement risk caused by time-zone differences
- Is real-time, uniquely secure, global and able to flex to meet the demands of a growing market
- Provides a multilateral netting process that improves liquidity and frees funds for further investment
- Reduces reconciliation costs and increases the efficiency of foreign exchange operations.

IT risk reduction measures
IBM and the settlement house have developed a very tight-knit relationship that enables both the business and IT to be managed through one virtual organisation. This reduces IT risk in a number of ways:
- The commercial relationship between the two companies means there are strong contractual aspects in place that enforce the controls necessary to manage risk
- There is increased audit supervision by IBM in addition to the normal business controls carried out by the client
- The settlement house has access to highly skilled, world-class resources in key areas such as security and IT resilience.

Business and IT operations are split between the UK and the US to spread risk geographically. This provides full business resiliency in the event of a regional disaster.

Designed with synchronous replication in mind, the settlement system is high availability with users of the service rarely seeing any business disruption due to IT issues. Very stringent SLAs are in place as part of the contract, enabling the settlement house to use its strategic partnership with IBM to improve the rigour and discipline around availability and service delivery.

The fact that the service levels in the contract are based on business metrics, not IT metrics, encourages alignment between business and IT objectives.

Quality of service is ensured through IBM’s well-established service delivery processes and regular reviews with the client ensure that quality is maintained.

The security features of the IT systems are very heavily audited. As the settlement house’s lead regulator, the Federal Reserve Bank carries out an audit of the service that IBM provides, the settlement house carries out its own audit and IBM audits itself.

The level of governance in relation to IT risk is extremely high at the settlement house because the entire business depends on IT. This is reflected in the high level of control and best practice testing methodologies built into the contract with IBM.
A complex route for many

Regardless of the obvious appeal it is clear that, for many financial institutions, achieving the demonstrable business benefits provided by the management of IT risk is not an easy task. The key challenges are cost, complexity and the availability of required skills.

The IBM Institute for Business Value’s recent survey of 25 financial institutions around the world illustrates Chief Risk Officers’ perception that large-scale IT expenditure will be required to control risk.

Against this background of perceived cost, there is also significant complexity associated with managing and further developing IT systems. The financial services sector has a history of acquisitions, partial improvements to systems and temporary fixes that eventually become permanent, which has led to infrastructures that are less than perfect. The specialisation, pace of information transfer and interdependence found in the sector have also created a network of extreme complexity.

For many financial institutions, this results in so many high severity issues across a diverse and interrelated set of platforms and architectures that identifying and resolving problems is a major challenge. So much time is spent fire-fighting IT problems that little or no time and resources are left for proactive risk management. Gaining access to the right skills to analyse and resolve these issues, and obtaining financial backing, is difficult given the constant pressure on costs. These factors compound the difficulties that already surround the assessment of operational risk in a company.

Transforming an IT risk profile – the first step

Assessing where an organisation is today is the obvious first step in transforming its IT risk profile. Through the experience of working with clients across a wide range of organisations, IBM has identified best practice in a number of areas and has developed the Maturity Profile shown in Figure 3. This describes a range of approaches that financial institutions are applying to their IT risk – from base level to best practice.

The settlement house previously referred to in the case study is a good example of an organisation that has achieved best practice.
## IT Risk Maturity Profile

<table>
<thead>
<tr>
<th></th>
<th>Base Level</th>
<th>Best practice</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business continuity</strong></td>
<td>Limited traditional disaster recovery plans drafted but not tested.</td>
<td>Disaster recovery plans in place for all applications and services, regularly tested.</td>
</tr>
<tr>
<td><strong>Geographic dispersal of operations</strong></td>
<td>People, operations and systems in same location. No separate physical disaster recovery site.</td>
<td>People, operations and systems geographically dispersed. Operations and IT with multiple data centres and delivery resource spread.</td>
</tr>
<tr>
<td><strong>Availability of IT applications</strong></td>
<td>Single instances of systems and data. Limited communication with intranet and extranet.</td>
<td>Some high availability systems configuration. Multiple communication links. Active—Active for all critical environments. Full redundancy. Synchronous replication.</td>
</tr>
<tr>
<td><strong>Quality of service delivery</strong></td>
<td>Limited documented service process and procedures.</td>
<td>Service delivery process and tools established to industry standard.</td>
</tr>
<tr>
<td><strong>Business architecture and IT architecture alignment</strong></td>
<td>Limited or no alignment between business and IT. Uncontrolled spend and development.</td>
<td>IT and business aligned with improved project governance and control of IT spend. Business IT change management established. Excellent interface and alignment between business and IT with dedicated IT business management. Full governance process in place for change to the environment.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Limited security controls and process. Limited security across the environment.</td>
<td>Established security policy with some testing and tools established to protect the environment.</td>
</tr>
<tr>
<td><strong>Governance – IT risk perception and engagement</strong></td>
<td>IT risk not perceived by CRO as key risk area to be managed holistically.</td>
<td>CRO is aware but delegates to CIO.</td>
</tr>
</tbody>
</table>

**Figure 3:** IBM Maturity Profile
Paths to achieving and accelerating benefits

The Maturity Profile demonstrates that there are various stages to achieving best practice and IBM has established methodologies that help organisations invest selectively in the areas that will provide maximum return on investment.

Rather than trying to achieve a transformation alone, however, there may be less risk of failure and the benefits may be achieved more quickly, by engaging a strategic partner with the right experience. While involving a partner extends the risk assessment outside the organisation, managed properly, the benefits can outweigh the risks. Across the financial services sector there is a great deal of experience of IT outsourcing that can provide a useful guide to best practice⁶.

Engaging a strategic partner can both increase the benefits gained from IT resilience and reduce the time taken to achieve them. A partner can also make risk management more affordable. Building and maintaining a complex, up-to-date IT infrastructure is prohibitively expensive, while sourcing from a partner provides usage-based pricing linked directly to the resources required.

The best strategic partners provide standardised technology platforms, tools, processes and test environments, enabling greater stability and end-to-end control for the financial institution. They can realise synergies by providing common regulatory compliance processes, reporting and data gathering. Moreover, staffing risk is reduced as the partner offers access to a large pool of expertise, lessening the likelihood of a loss of requisite skills, while at the same time reducing staffing overheads and costs. All these benefits are realisable in a shorter timeframe and at less cost than would be possible through a standalone strategy.
Conclusion

All financial institutions have to manage risks; it is both a regulatory duty and a business imperative. While IT can represent a significant risk to an organisation, managed well, there are many benefits to be gained.

A combination of high profile threats, a growing regulatory burden and the rising cost of risk management is placing increasing focus on operational risk and the central role that IT plays in managing risk throughout an organisation. When taking action to control risk, it is important to understand how to assess IT risk, to apply best practice and to monitor and measure the results achieved.

To access publications on related topics or to browse through other materials for business executives, please visit our website:

ibm.com/easyaccess/ukfinancialservices
Authors

Nigel White
Strategic Services Engagement executive, IBM Global Technology Services
nigel_white@uk.ibm.com

Marc Jones
Financial Services executive, IBM Global Technology Services
marc_jones@uk.ibm.com

Mike Brookbanks
Executive IT architect and Principal, IBM Global Technology Services
mike_brookbanks@uk.ibm.com

Jessica Douglas
Business Consultant, IBM Global Business Services
jessica.douglas@uk.ibm.com

Reference documents

Referenced documents are available from any of the authors whose contact details are shown above.

1. Current regulatory environment in banking (Market Focus), Datamonitor, ref: BFTC1271, March 2006
2. Digital Risk – the Challenge for the CRO, The Economist Intelligence Unit, James Watson and Gareth Lothhouse, September 2005
5. Zurich Strategic Risk, Measuring and Rewarding Business Resilience, Malcolm Stokes and Mark Platten, AIRMIC Conference 2004
6. Successful Sourcing Strategies, Mercer Oliver Wyman, white paper 2006