



White Paper: What has the recession taught us about operational risk and resilience?

Keeping people and information **connected**



ICAEW
INFORMATION
TECHNOLOGY
FACULTY

SUNGARD[®]
Availability Services

TITLE: What has the recession taught us about operational risk and resilience?

AUTHOR: A SunGard Availability Services Whitepaper

Word count: 2,500

<http://www.sungard.co.uk>

FOREWORD

Resilience and robustness are words which now play a dominant part in any discussion on business best practice. Whether the focus is financial performance, the supply chain or information technology (IT), resilience and robustness are now viewed as being absolutely crucial to the success of any organisation.

Whilst most commentators have focused on the need for financial resilience in the face of the increased risks associated with the economic downturn, the area of operational risk and resilience has been transformed dramatically as a result of the recession. Many businesses have experienced business problems not because they themselves have created a problem but because a partner or supplier has caused a problem through unavailability of resources and/or staff.

The ICAEW IT Faculty hosted an event in June 2009 in conjunction with SunGard Availability Services, exploring the theme of Risk and Resilience in a Recession. The discussion provided insights into businesses' attitudes towards risk management and resilience planning, and the impact that the economic downturn has played in highlighting the range and severity of threats that CEOs, CFOs, CIOs and other business leaders need to prepare for and protect against.

In conjunction with this event, a poll of a group of Institute members examined how perceptions of operational risk have changed in light of the recession. For instance, resilience planning is no longer just about keeping the business up-and-running in the event of incidents such as a flood or fire. Now organisations are focusing on understanding the exact flow of information through the business; identifying which information is mission-critical and ensuring that they have resilient – and streamlined – infrastructure in place to access this information at all times, from any location.

Another interesting finding in our poll was the importance attached to risk management and resilience within organisations. Previously considered to be firmly within the domain of the business continuity manager or the IT manager, responsibility for resilience planning is now distributed across various roles and functions, and is often now a topic for discussion within the Board room.

Technology continues to play a critical part within risk management and, despite the recession and the need to strip back costs, organisations continue to spend money on technologies to support and backup their operations. Increasingly, this involves outsourcing to specialist third parties which offer a cost-effective level of resilience hard to achieve internally, leaving the IT department more able to focus on strategic innovation to help the business grow.

No organisation can ever be 'fully resilient' – such is the unexpected, unpredictable nature of risk that no company can ever be 100 per cent confident that it is protected against any eventuality. However, what we are certainly seeing is that resilience is becoming far more of a focus for nearly all organisations as business leaders recognise that information (and IT systems) lie at the heart of everything that they do.

Customers, suppliers, staff and shareholders need to know that an organisation is doing all it can to manage risk and therefore, during this time of great economic uncertainty, it is perhaps no surprise that resilience has become a very major focus within business.

John Oates, Chairman of the IT Faculty, ICAEW

A RISK VS RESILIENCE ENVIRONMENT

The economic crisis has not surprisingly led to a heightened sense of risk amongst consumers and businesses alike. Daily reports of government takeovers, firms going bust and large-scale redundancies concern everyone in society.

Businesses are facing increased financial risk in the current economy but what is now clear is that organisations are also finding themselves at greater risk in terms of their day-to-day operations. At the discussion held at the ICAEW's IT Faculty, attended by CFOs and Heads of Operational Risk from a number of large organisations within the UK, it was evident that business leaders are constantly having to examine and revise their resilience plans in line with the rapidly-changing economic environment.

Looking at the broader picture, we believe that there are five major factors currently shaping the way in which businesses approach risk management and resilience:

- 1. Political and corporate instability brought about by the economic downturn has brought with it a heightened sense of operational risk for organisations.** Disasters do not stop in a recession; if anything, the associated risks increase as corners are cut and reduced workforces have to pick up more responsibility. Inevitably, problems arise.
- 2. Organisations are required to process, store and secure rapidly increasing amounts of data, which itself poses a huge risk.** Understanding information flow within an organisation and ensuring that mission-critical data is available at all times is essential for true operational resilience. Many companies now use IT as a competitive differentiator against their rivals. The ability to access data, and, more importantly, critical information, by staff making intelligent decisions is essential in today's economic environment. It follows that, with a higher awareness of risk, any reports of downtime, or even the most minor operational problem, can be exaggerated and paint a picture of a business that is not taking risk management seriously and does not possess sufficient levels of resilience.
- 3. Outsourcing has been widely embraced as a way for businesses to streamline operations whilst maintaining levels of service.** Organisations are becoming increasingly rigid in terms of where they want to focus their resources, namely their core business operations. Other business functions are considered a distraction, so outsourcing has become the way around that.
- 4. The 'domino effect' of supply chain problems means that every organisation is at risk from the recession, both in terms of financial performance and operational continuity.** The example of Zavvi, the entertainment chain, at Christmas 2008 in the UK, highlighted the consequence of an insufficiently robust supply chain and a thorough understanding of all key suppliers. Following the collapse of Woolworths, Zavvi, which relied on Woolworths' distribution arm, Entertainment UK, to supply its DVD, CDs and computer games, was forced to shut part of its website and cancel orders, and this eventually led to the company going bust.
- 5. Limited capital investment in many organisations makes 'manual' services more attractive to CFOs.** As an alternative to this, within the IT function, software, hardware and storage 'as a service' (XaaS) – purchased on a 'pay-as-you-go' basis, is becoming increasingly popular and may help businesses to maintain a healthy balance sheet.

TRENDS WITHIN RISK MANAGEMENT

The business operational risk landscape has changed considerably during the current economic recession. The ICAEW poll carried out in June 2009 found that almost two thirds of members believe that levels of operational risk have increased within the past year. Experience shows that it usually takes major incidents such as the London terrorist attacks of July 2005 or the summer flooding of 2007 to bring about such heightened perceptions of risk. In a recession, however,

organisations are far more aware of the mundane, everyday risks that can have crippling consequences on normal business operations, such as supply chain problems, a power outage or redundancies.

- **Supply chain risk**

The ICAEW poll found that 70% of respondents believe they are at more risk from damaging supply chain issues (e.g. business partners going out of business) than they were a year ago. This increased risk is aggravated further by the shift towards outsourced business functions referred to above. As entire business departments and critical IT infrastructure such as storage and communications are outsourced to third parties, organisations open themselves up to huge risks should these suppliers run into trouble.

Therefore, it is imperative that organisations select outsourcing partners with due diligence. The British Standards Institute recognised the need to provide more assistance to businesses concerned about the impact that a problem within their supply chain could have on their own operations by introducing Business Continuity Management Standard BS 25999. This Standard gives businesses an indication that a particular supplier is following certain business continuity guidelines and practices and it is likely that further initiatives such as this will follow in the near future. However, in the recession, organisations have had to go beyond this and assess on a regular basis whether the supplier in question is still likely to be operating as a going concern in a year's time.

- **Redundancies**

As organisations, particularly within the financial services sector, have looked to cut expenditure and reduce headcount, they have faced a variety of relatively new operational risks. The first of these, and certainly the most obvious, is that of departing employees looking to maliciously cause damage to the business' operations as a means of enacting 'revenge' on the employer. Incidents such as these are hard to prevent and protect against, and many organisations struggle to find the right balance of approach when dealing with departing employees.

On the other hand, organisations have also had to face up to and protect against another risk caused by wide-scale redundancies, namely the risk of knowledge departing the company or loss of Intellectual Property. If an employee that is responsible for a crucial element of the day-to-day operations of the business is made redundant, organisations need to ensure that all of his or her knowledge, relevant experience, and relationships with partners and suppliers, is passed on effectively, otherwise the organisation becomes less resilient. This is particularly true if an employee such as a business continuity manager or risk manager is made redundant.

Over half of respondents to the ICAEW poll believe that redundancies have impacted on the effectiveness of day-to-day operations and increased operational risk. For this reason, many organisations are now acknowledging the benefits of using risk management and business continuity software to properly document resilience planning, ensuring information is captured within the company's IT systems, rather than in one person's head.

- **Increased investment in IT**

Tightening regulation and growing volumes of data are driving institutions to invest significant sums in expensive IT and data centre capacity: according to the Digital Realty Trust, corporate data centre requirements have grown by over 20 per cent during the past year alone. The Digital Britain report of June 2009 stated that the data centre sector must strive to build more data storage facilities in the UK if it is to meet growing demand.

The ICAEW poll showed that organisations expect to increase investment in network infrastructures, servers and security over the next 12 months, despite the need to streamline

operations. Wherever they can, IT departments need to do more with less, accommodating more applications and data, without compromising the resilience of the business.

TRENDS WITHIN RESILIENCE PLANNING

Over the past 18 months we have seen a dramatic shift in the approach that leading organisations are taking towards resilience planning. Most noticeable is the sea-change in thinking when it comes to ensuring data centre and technology resilience. Whereas the vast majority of organisations previously looked to keep as much of their risk management and resilience planning in-house, believing that to be the most effective and secure approach, most are now favouring a *managed services* approach.

At the heart of this trend is the recognition by many corporations that the most 'unexpecteds' can be planned for and embedded within a resilient IT infrastructure that spans both in-house corporations' IT departments and partners. In addition to this, there need to be plans to handle extreme unexpected incidents that require corporations to give key staff an alternative place from which to operate.

- **The outsourced data centre**

In the pursuit of maintaining a lean balance sheet with optimum cash flow, boards are paring back on new capital investments (CapEx), opting wherever possible to fund projects from operating expenditure (OpEx) instead, and acquiring new capabilities as managed services. When this approach is brought to bear in resilience and data centre strategies, the benefits are extremely attractive to all organisations. Indeed, with data centre investments generally written down over ten years – an eternity in technology terms – the managed services approach makes compelling business sense from both a cost and capacity perspective.

However, the most important considerations for CIOs, when it comes to outsourcing the business critical IT functions held within a data centre, concern the overall security and resilience of the managed service provider's facilities. Handing over data centre operations to a specialist third party does not offer resilience in itself. Not only should individual facilities offer total resilience, the managed service provider should also have a network of resilient facilities to provide total failover in the event of a major disaster impacting the primary data centre. A single site is never resilient, no matter how advanced its technology. Given the sensitivity of the data businesses hold, it is also vital that any managed services provider can provide complete backup and recovery services in the event of data loss.

- **New technologies**

As organisations embrace virtualisation technologies and cloud computing to cut costs and allow them to focus on profit-generating activity, managed services providers assist with the transition to these new models of computing, ensuring *always on* availability and security. These 'intelligent hands' perform a vital role. Not only do they ensure the systems function at optimum levels, they also allow CEOs to keep their own teams focused on the services and systems the institution manages for itself, with no dilution of resources.

Virtualisation has signalled the biggest change in the way that large organisations approach computing within the past five years. According to IDC, spending on virtualisation software and services is expected to exceed \$15 billion worldwide by 2011. The desktop virtualisation market alone will make up \$2 billion of that total. And, sales of virtualization management software are set to hit \$2.7 billion this year.

The term 'virtualisation' broadly describes the separation of a resource or request for a service from the underlying physical delivery of that service. For instance, platform virtualisation separates an operating system from the underlying platform resources. With virtual memory, computer software gains access to more memory than is physically installed, via the background swapping of data to disk storage. Similarly, virtualisation techniques can

be applied to other IT infrastructure layers - including networks, storage, laptop or server hardware, operating systems and applications.

Virtualisation dramatically improves the efficiency and availability of resources and applications in an organisation. Internal resources are underutilised under the old 'one server, one application' model and IT administrators spend too much time managing servers, rather than innovating. An automated data centre, built on a virtualised platform, lets organisations respond to market dynamics faster and more efficiently than ever before. The best virtualisation platforms deliver resources, applications – even servers – when and where they're needed.

We are now likely to see an upsurge in the numbers of major corporations adopting cloud computing, whether that be through so-called private clouds (which allow businesses to keep control of their own critical data) or external clouds, where data is hosted by third parties in their own data centres. In discussion of cloud computing among large businesses, the inherent risk associated with placing data outside the company firewall, is often raised as an issue. Organisations will demand complete security in the external cloud; if suppliers do not provide this, it is likely that the subsequent vulnerabilities will force many organisations to retreat from the cloud.

- **Resilience on the Board agenda**

The ICAEW poll revealed that resilience planning is now firmly established as a crucial aspect of business. At the ICAEW event on *Risk and Resilience in a Recession*, one risk manager at a large multinational company stated that he now finds it much easier to secure budget for resilience, simply by saying to the CFO that the particular initiative in question is 'in support of Business Continuity Planning'.

Almost a third of respondents responded that resilience is discussed at Board meetings and over 80 per cent said that it is discussed at Operations Board meetings. Around 10 per cent of organisations actually discuss resilience in customer fora, and this number is likely to rise, reflecting the heightened sense of risk that both individuals and businesses currently feel.

Whereas five years ago, business continuity and disaster recovery was very much the preserve of the IT department, the growing necessity for 24/7 information availability has meant that resilience and risk management has expanded across all functions within the organisation. Therefore resilience needs to be controlled and managed at the very highest levels of the business and most large organisations now have at least one person, if not a team, overseeing all aspects of resilience planning.

- **A lack of testing**

One more negative trend within resilience planning during the recession has been a decrease, albeit slight, in the numbers of contingency plan tests being carried out. This undoubtedly stems from wide-scale cost cutting across the business but does highlight a worrying belief that still exists that business continuity testing is something that is optional. Experience has shown that contingency planning must be embedded into an organisation's culture on a day-to-day basis to be truly resilient.

MOVING FORWARD

Clearly, the recession has certainly helped to bring the whole issue of operational risk management and resilience planning to the forefront of the business agenda. Organisations, and individuals at the very highest levels of decision-making within them, have recognised that they simply cannot afford any downtime in such tough economic conditions. What is more, these organisations are starting to recognise the benefits of understanding the exact nature of the information that flows through them and the competitive advantages and cost savings that can be gained through sound resilience planning. The current shift towards data centre outsourcing and

managed services is one area where organisations are able to increase resilience, whilst streamlining processes, freeing up staff time and reducing capital expenditure.

In the coming months and years, we will witness those organisations that have streamlined their operations and processes during the recession, and taken the opportunity to hand over resilience to third party experts, in a position to steal a march on their rivals as the economic recovery gathers pace. This recession has taught us many things but surely one of the most worthwhile lessons has been that organisations can no longer afford to neglect operational risk management; the businesses that win in the coming decades will be the ones that understand the digital age we now live in and have the resilience in place to serve their customers, no matter what.

For practical insights into business risk, continuity and information availability, the complimentary report '[From Adversity to Availability](#)' may be requested at: www.a2areport.co.uk

SunGard Availability Services provides disaster recovery services, managed IT services, Information Availability consulting services and business continuity management software to more than 10,000 customers in North America and Europe. With five million square feet of datacenter and operations space, SunGard assists IT organisations across virtually all industry and government sectors prepare for and recover from emergencies by helping them minimise their computer downtime and optimise their uptime. Through direct sales and channel partners, we help organisations ensure their people and customers have uninterrupted access to the information systems they need in order to do business. Representing Intellect, the trade association, on the steering committee for BS 25999, SunGard helped to define the business continuity management standard. *Continuity, Insurance & Risk* has recognised SunGard as service provider of the year an unprecedented six times.

Availability Services is a division of SunGard Data Systems, the largest privately held business software and services company on the Forbes list of private businesses, serving more than 25,000 customers in more than 70 countries, including the world's 25 largest financial services companies. With revenues of \$5.6 billion, a 21% CAGR and 10% organic growth, SunGard has enviable financial strength. Visit SunGard Availability Services at www.sungard.co.uk

As a world-class professional accountancy body, The Institute of Chartered Accountants in England and Wales (ICAEW) provides leadership and practical support to over 132,000 members in more than 160 countries, working with governments, regulators and industry to maintain the highest standards.

Our members provide financial knowledge and guidance based on the highest technical and ethical standards. They are trained to challenge people and organisations to think and act differently, to provide clarity and rigour, and so help create and sustain prosperity. The ICAEW ensures these skills are constantly developed, recognised and valued.

Because of us, people can do business with confidence.

SunGard Availability Services

SunGard Availability Services keeps people and information connected, preventing business interruption. As pioneers of Information Availability since 1978, our experience across all business sectors, environments and platforms is unrivalled. With a wide range of secure, scalable solutions only SunGard has the breadth of resources and expertise to keep your organisation's people, IT infrastructure and data available no matter what.

Consulting

We help you get risks under control, thereby safeguarding your profits, operations, customers and reputation by leveraging our industry-acknowledged operational risk management expertise. From business continuity management to the full lifecycle of technological solutions, we deliver results unique to your business because our start point is always your business needs.

Recovery Services

Interruptions to business are difficult to predict, but SunGard customers know that when disaster strikes, they are always ready. With the widest range of effective solutions SunGard ensures that any business impact is minimised, returning you quickly back to business as usual.

Managed Services

SunGard's Managed Services give you the IT resources and skills you need to ensure availability, reliability, security and cost efficiency. Yet we leave you in full control of the systems, applications and data that drive your business forward.

BCM Software

Our market-leading suite of BCM Software allows you to develop a world-class BCM regime, to manage your preparedness, and any business interruptions you experience. It ensures your staff and customers are fully informed, and that the right people and resources are deployed at the right time.



Information Availability you can trust

SunGard Availability Services understands how vital Information Availability is to protecting key operations, servicing customers, preserving reputation, maintaining profitability and engendering stakeholder confidence. Over 10,000 customers trust us to keep their people and information connected. Trust us to do the same for you.

t: 0800 143 413

e: infoavail@sungard.com

w: www.sungard.co.uk

United Kingdom & European Head Office

12-13 Bracknell Beeches, Old Bracknell Lane West,
Bracknell, Berkshire RG12 7BW

SUNGARD®
Availability Services

Keeping People
and Information
Connected.

Consulting

Recovery
Services

Managed
Services

BCM
Software