Deloitte.

# Navigating the journey
# Financial Services: Heads of IT Risk Survey 2013

July 2013

# Contents

# Introduction

The financial services industry continues to feel the pressure. Sustained regulatory attention, a sharper focus on shareholder value and customer service, coupled with an ever more competitive and closely scrutinised market are paving the way for much needed transformational change. Information technology has emerged as a key enabler to deliver this change, yet the resulting risks posed to organisations are on the rise.

Our previous survey, ‘Heads of IT Risk: Directing a new function’, showed how IT Risk functions originally emerged following improvements in risk management practices across the organisation.

Two years on, the IT Risk function has evolved, growing in size, responsibility and with higher executive visibility. These factors, combined with heightened regulatory focus, constrained budgets, and a struggle to find people with the right skills, have created a challenging environment.

This survey brings together insights from IT Risk functions from twenty of the largest global financial services institutions. Undertaking face-to-face interviews with those responsible for setting the IT Risk agenda allowed us to get an inside view into the challenges facing IT Risk in the financial services industry as it navigates its way through testing times.

# IT Risk in the headlights

Engaging in active dialogue with the regulator will enable IT Risk functions to better align themselves to the behaviours and actions regulators are demanding. Over time, this will lead to a situation where regulator focus becomes the norm.

## Heightened regulatory focus

In the UK, the Financial Conduct Authority (FCA) has cited technology as one of its five priority risks for 2013/14[1]. Other recent regulatory stipulations, such as the FSA's 'Dear Chairman' letter requesting businesses consider resilience when changing or designing IT systems and processes, has added to the pressure put on IT Risk functions. Our survey indicates that the majority of IT Risk functions feel this increased regulatory scrutiny has, and will continue to, significantly impact their business as usual activities.

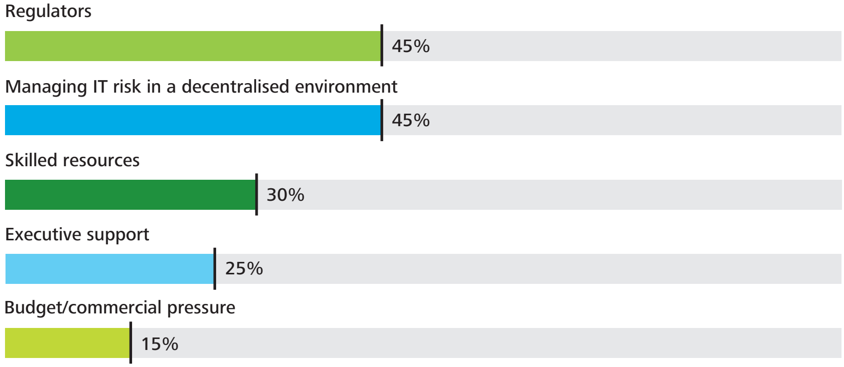
When asked where the greatest challenges lie over the next twelve months, unsurprisingly, regulation was the most common response from survey participants, with forty-five per cent citing it as a key challenge in achieving their IT Risk objectives (figure 1). The shared sentiment is that regulators are more visible and are playing a key role in shaping the direction of travel as they are becoming more prescriptive in their requirements.

Nearly half of survey respondents believe that interfacing with regulators is a key area of responsibility for IT Risk functions (figure 2). The more mature functions are building relationships with the regulators directly to get an early view of upcoming regulatory change and to help shape the direction through the consultation process.

Despite seeing the benefit in working more closely with the regulators, many of our survey respondents felt that there was still a need to overcome 'a lack of pragmatism', 'unrealistic expectations' and the 'sheer volume of requirements from multiple regulators'.

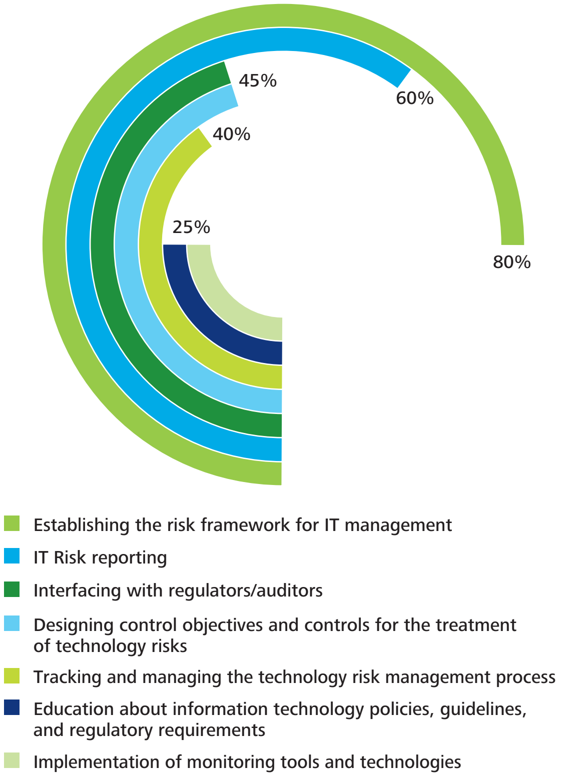
[1] Financial Conduct Authority. (2013). Business Plan 2013/14. London: Financial Conduct Authority

**Figure 1. Top challenges in achieving IT Risk objectives**



(percentages based on top answers given)

**Figure 2. IT Risk function areas of responsibility**



> "A significant proportion of our budget has to be allocated to address new regulatory requirements."

Head of IT Risk, Global Investment Bank

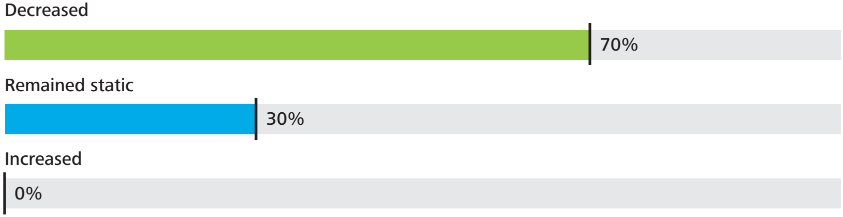
Whilst an increased profile brings increased strength to the IT Risk function, it is key that setting the IT Risk agenda remains in its control.

## Increased executive attention

**Informed opinion is unequivocal; IT Risk has never been higher on the executive agenda. Our survey tells us that organisational risk appetite is decreasing year-on-year, with seventy per cent of our respondents citing a reduction in the last twelve months, increasing the executive pressure and focus on IT Risk (figure 3).**

C-suite focus on IT Risk is at an all time high and this attention has resulted in a significant increase in the number of IT Risk functions that are engaged directly by the Board to report, update or provide direction on IT Risk matters. Retaining and developing this executive support will be seen as a key opportunity for IT Risk functions over the next two years.

**Figure 3. Changing risk appetite over the last 12 months***



**1 January 2012 to January 2013*

# Missing signposts

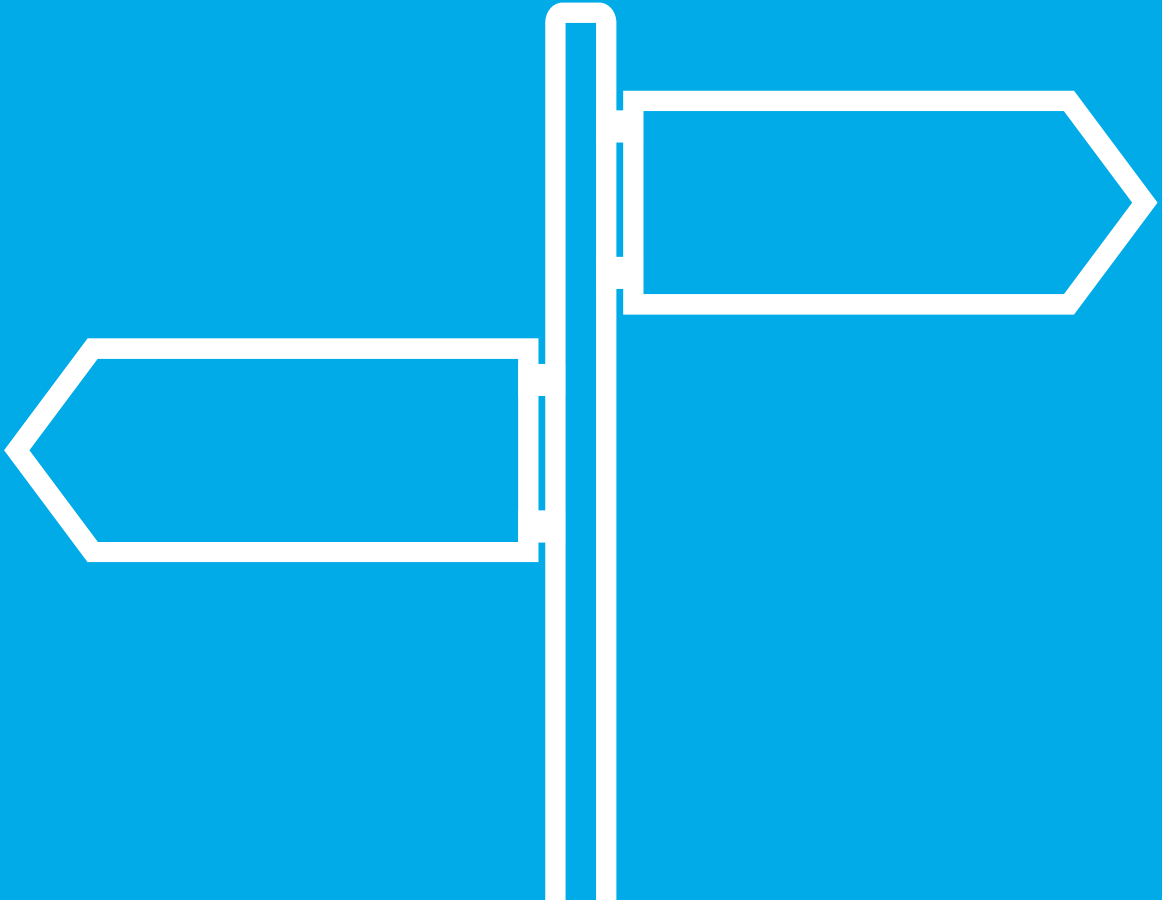
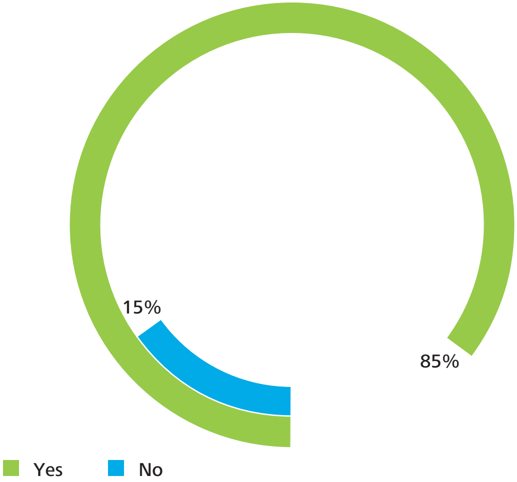


**Figure 4. Is it a challenge to produce data-driven Management Information?**



> "Putting IT risks into the context of business risks and opportunities has not been a strength of the technology risk function historically."

Head of IT Risk, UK Retail Bank

**Eighty-five per cent of organisations identified challenges in producing comprehensive data-driven Management Information (MI) to enable timely, accurate and relevant decisions.**

## Catering for the executive

Where IT Risk is reported to a senior level, considerable effort is required to present this information in an executive-friendly format.

Our survey respondents highlighted challenges across the financial services industry in producing consistent, transparent data in line with business requirements and on a timely basis.

## Lacking the right tools for the job

The majority of respondents indicated that there was a large degree of manual effort required to generate regular reports. Organisations spend a considerable amount of time working around the data they have, rather than designing data, reporting and tools to suit their needs.

## Looking ahead

Effective MI allows organisations to identify and escalate issues either as they arise, or before they are realised. Yet many respondents indicated a low level of maturity in their ability to identify risks proactively, with only fifteen per cent believing their IT Risk reporting was proactive and dynamic (figure 4).

Those on the front foot are harnessing their MI to build emergent capabilities in proactive education, awareness and forward-looking risk assessments.

# A shifting role

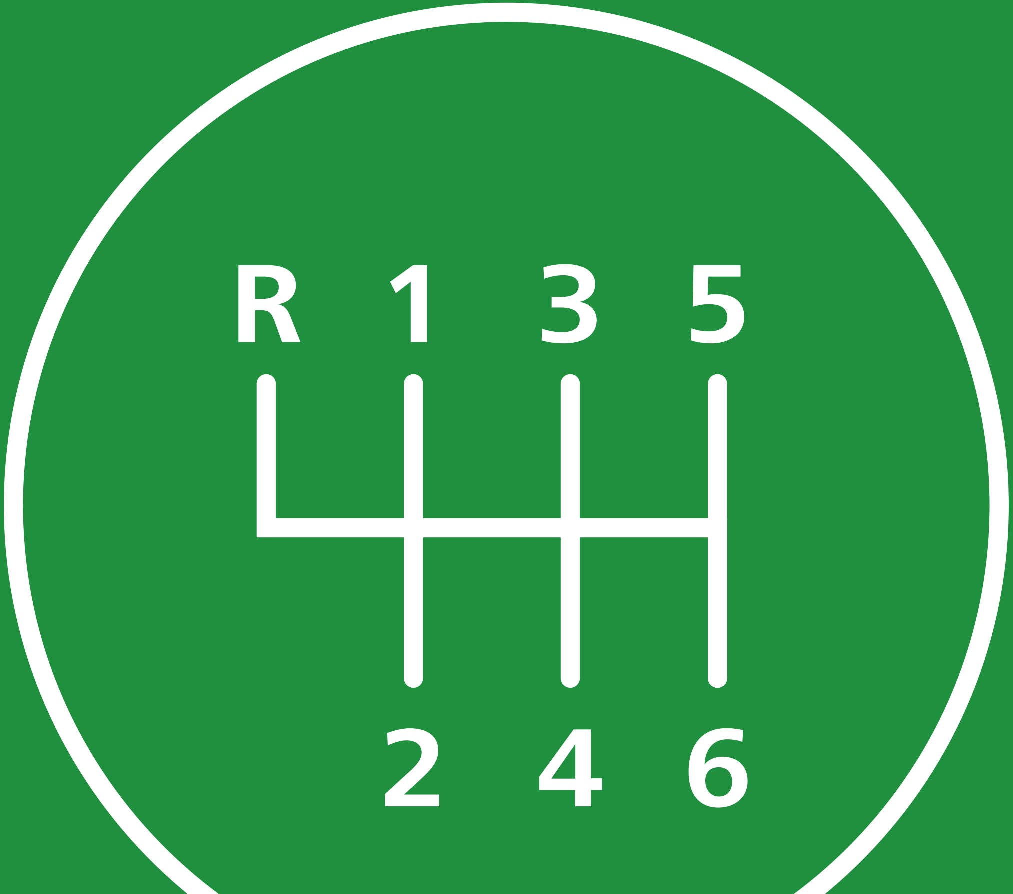
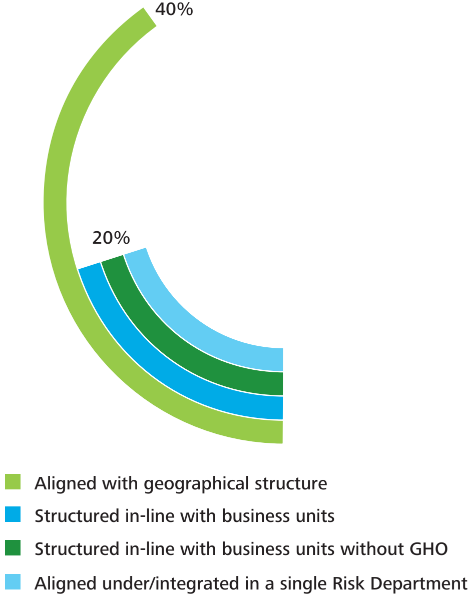


Figure 5. IT Risk function structure



Heightened executive attention has led to an increased set of roles and responsibilities and IT Risk functions are positioning themselves more and more in the second line of defence, forcing the front line to take responsibility for control operation.

## A structural change

An increase in roles and responsibilities has led to a structural shift for many IT Risk functions. Sixty per cent now adopt a ‘hub and spoke’ model, where a central function sets strategic direction and policy, and geographically dispersed IT Risk teams bring local insight and experience to delivery. Typically, this approach is seen in the larger retail banks and global insurance groups.

Twenty per cent still rely on a more traditional model of having a light central function setting strategic direction and having limited day-to-day interaction with front line control and operational functions. This is typically where the organisational risk culture is more focussed on credit, financial and market risks rather than technology, and our survey suggests this is more common across the investment management and insurance sectors.

> “I was previously seen as the security person perhaps with responsibility for some other related areas, I am now the IT Risk person with security being just one of these areas.”

Head of IT Risk, Multinational Investment Bank

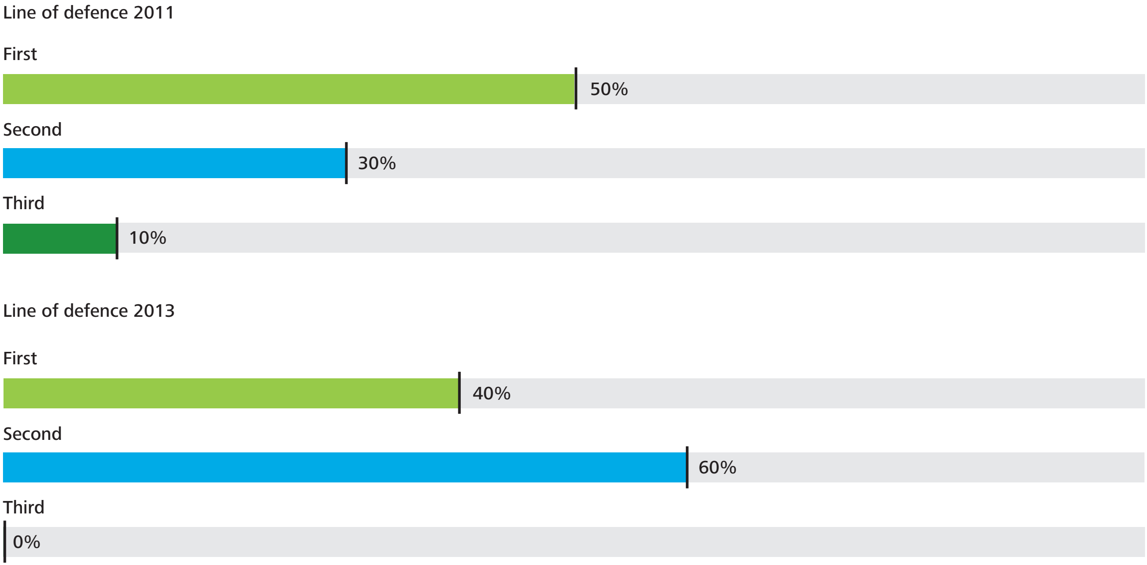
## Lines of defence

The majority of respondents have a clear ambition to operate in their organisation’s second line of defence, giving accountability for control design and operation to the front line. Our survey results show a marked increase in IT Risk functions moving from the first line to the second line of defence (almost two-thirds now operate in the second line compared to just thirty per cent in 2011).

Despite this seemingly rapid transition, it has not been without challenges. All functions that saw themselves as purely second line highlighted the on-going challenge to interact with the front line in an effective manner – citing issues ranging from the inability to gain traction, to overreliance on the IT Risk function. Nearly all respondents mentioned the continued challenges around extricating themselves from legacy arrangements, such as control operation and providing detailed Subject Matter Expertise (SME) input to control design.

This was compounded in organisations going through a restructure or global expansion, where control ownership and responsibility were in a state of flux.

**Figure 6. Position of the IT Risk function in the lines of defence model[2] (2011 to 2013)****



[2] As quoted by the Institute of Internal Auditors (IIA), the first line of defence is management control, the second line of defence is supported by various risk control and compliance oversight functions, and the third line of defence is internal audit. *Source: IIA (2013). Position Paper: The three lines of defense in effective risk management and control. Florida: IIA Global*

# Running on empty

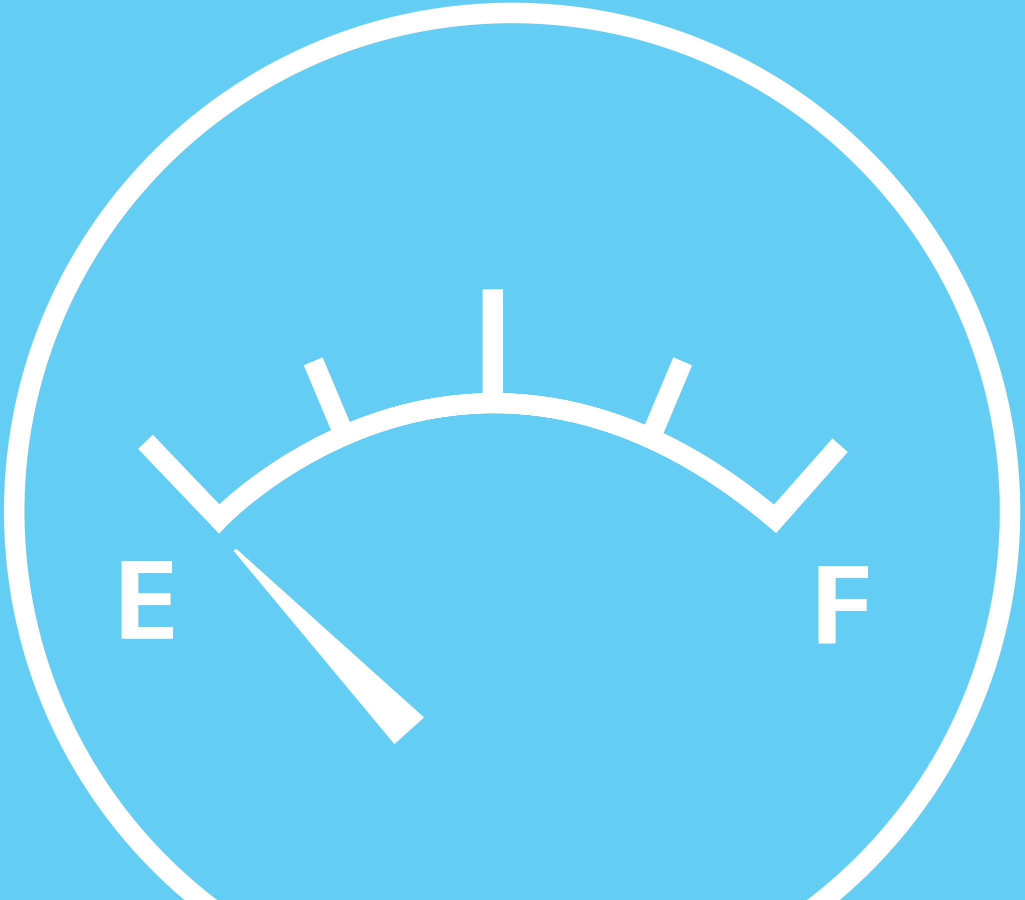
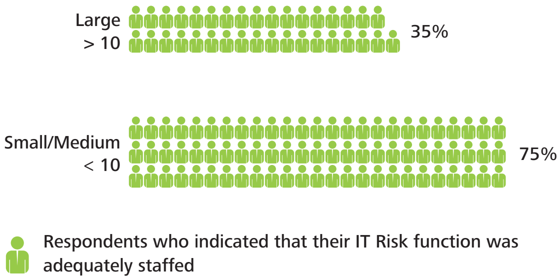


**Figure 7. Headcount sufficiency in relation to IT Risk function size**



Senior stakeholders’ expectations of an organisation’s risk management capability continue to grow, yet the challenge to effectively resource departments with the right balance of people and skills is proving a significant challenge.

## We’ve got skills, just not the right skills

As the IT Risk function expands its remit, influence and exposure, there is a need to develop its skillset from traditional technical capabilities to a broader base, incorporating strategic decision making, programme management and senior stakeholder engagement. Nearly a third of survey participants identified a lack of skilled resources in the market as a top challenge in achieving their objectives. Interestingly, this number increases for larger functions (more than 10 employees) where nearly two-thirds noted the skills shortage as a key limiting factor.

## The larger the function, the tighter the squeeze

Whilst seventy-five per cent of small functions thought their headcount was sufficient, only a third of larger functions agreed (figure 7). This may be because larger risk functions have a broader risk management remit where roles and responsibilities are rapidly changing, whereas smaller functions commonly have more limited objectives, often restricted to policy setting and remote oversight.

## Plugging the gap

With a shortage of skills, organisations are looking to secure the right resources by alternative means. A high proportion of functions outsource IT Risk activities, providing faster access to the right skills and increasing flexibility compared with sourcing from within the organisation, as is the more conventional approach.

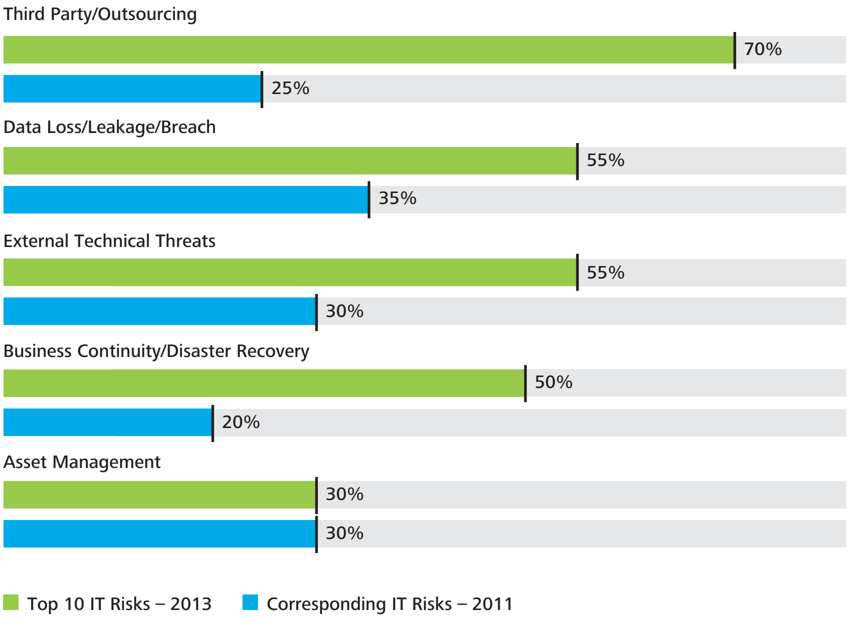
# Knowing the hazards

**Recent high profile and material failures in IT control have centred on 'traditional' IT risks such as business continuity, data loss, change management and third party suppliers. Despite the hype around certain risks, such as social media and bring your own device (BYOD), it is the more traditional risks that are still making the headlines.**

This may explain why our 2013 survey shows no change in the top five IT risks since 2011. In fact, with the on-going and rapid developments in technological capability, usage and penetration, our respondents were even more concentrated in their view of the top risks than in 2011, when there was a wider spread.

If the IT Risk function is to add value to the business, it needs to keep executive awareness focused on the right risks for their organisation, rather than primarily those that are in the public domain.

**Figure 8. Comparison of top IT Risks faced by Heads of IT Risk in 2011 and 2013****



> "If you throw me in the snake pit, the first thing I want to know is which ones are poisonous."

Head of IT Risk, Global Investment Bank

### 1. Third Party/Outsourcing

Seventy per cent of respondents identified third parties and outsourcing as a top risk, a significant increase from 2011. Yet despite all organisations engaging with third parties, only half of IT Risk functions play an active role in supplier selection and on-going supplier assurance, reducing the function's ability to control and influence the associated third party risks.

### 2. Data Loss/Leakage/Breach

High profile data leakages continue to cause significant adverse publicity and regulatory sanction to those organisations affected. Although the industry invests significantly in data leakage prevention and detection technologies, over half of our respondents still see this as a key risk to their organisation.

### 3. External Technical Threats

Technical threats, such as cyber attacks, are becoming increasingly sophisticated and there is a growing trend for hackers to use 'collectives' to pool knowledge and resource to mount targeted and sustained attacks. The number of respondents indicating that this was a key risk to their organisation has nearly doubled since 2011.

> A consolidated view of IT Risk can only be gained if the risk exposure posed by the extended enterprise is fully understood.

### 4. Business Continuity/Disaster Recovery

Recent technology failures across the industry have brought business continuity to the fore. As a subject of significant regulator interest, it is unsurprising that half of our survey respondents have named it as one of their top IT risks for 2013. Despite the investment in disaster recovery, its usage often remains a decision of the last resort, leading to regulators and senior executives starting to ask the question 'why?'

On top of this, the risk of a major cyber event is sharpening focus on resiliency and the interface between technology incident management and business crisis management.

### 5. Asset Management

Insufficient control around corporate assets can have a direct impact on the bottom line. Focus on the protection of these assets, such as laptops, mobile devices and IT infrastructure, has ensured that IT Risk functions still see this as a core area of focus, despite other risks being of a 'higher profile' and in the public domain.

> "…based on our analysis of existing attacks, [cyber criminals] are just trying to make a point – this is about disruption for visibility. If they really wanted to take us out, they could."

Head of IT Risk, Multinational Bank

# Final thoughts

This year's survey results have demonstrated how the pressures on IT Risk functions have increased. Having a wider remit means a Head of IT Risk must wear multiple hats, whilst heightened executive attention also means delivering under intense scrutiny from the Board. The external challenges are also adding to the heat, with increased regulatory visibility and a shortage of skills in the market to deliver on the demands of their organisations.

So what does the future look like for the IT Risk function within financial services organisations? Gauging from the survey responses, we have drawn out the following key points that we believe will be instrumental in shaping the future direction of the function.

01

Getting on the front foot with the regulator is key to helping shape, plan and prepare for upcoming regulatory change.

02

Now that the executive spotlight is on IT Risk, developing and fostering that executive engagement will be critical to ensuring IT Risk remains high on the agenda going forward. Focusing on forward-looking MI will be a key driver in developing this relationship, allowing for real risks to be positioned in a business context and understood by the executive.

03

As roles and responsibilities mature, it is key that IT Risk functions remain agile to changes in demand for skills, headcount and organisational structure to tackle new focus areas and potential hazards.

04

Whilst emerging risks often grab the headlines, maintaining organisational focus on areas of highest risk (such as supplier selection, assurance and traditional IT controls) is vital if organisations are to overcome the fundamental and material IT failures experienced by the financial services industry in recent years.

**Acknowledgements**
We would like to extend our thanks to those Heads of IT Risk in the financial services industry who contributed to this survey.

**The data used for year-on-year comparison in figures 6 and 8 was taken from a similar sample of financial services organisations that carried out our 2011 survey: ‘Directing a new function’.

# Contacts

**Chris Recchia**
Partner, Financial Services
+44 (0)20 7007 5159
crecchia@deloitte.co.uk

**Tom Bigham**
Technology Risk Management
+44 (0)7917 084 327
tbigham@deloitte.co.uk

For more information, visit www.deloitte.co.uk/itrisk

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.co.uk/about for a detailed description of the legal structure of DTTL and its member firms.

Deloitte LLP is the United Kingdom member firm of DTTL.

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication. Deloitte LLP would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte LLP accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom. Tel: +44 (0) 20 7936 3000 Fax: +44 (0) 20 7583 1198.

Designed and produced by The Creative Studio at Deloitte, London. 28152A