

# IT Risk – Closing the Gap

Giving the Board what it needs to understand, manage and challenge IT risk



# Contents

Foreword	1
Executive summary	3
Survey findings	
Does the Board fully understand the impact that IT risk can have on the business and the need for assurance?	5
Does Internal Audit provide assurance in the areas that the Board needs? Where does Internal Audit focus its efforts?	9
Does Internal Audit have the credibility and capabilities to deliver assurance to the Board?	15
Appendix	19
About the authors	21

# Foreword

The risks related to the use of information and communication technology (IT), including IT project and IT security, are increasingly on the Board's agenda. The Institute of Internal Auditors – UK and Ireland (IIA) engaged PricewaterhouseCoopers to conduct research in this area, focusing on the views of senior managers and Heads of Internal Audit, with the aim of establishing their perception of IT risk and the level of assurance that Internal Audit specifically provides. The conclusions from this survey will be used to shape the Institute's education strategy going forward.

A major emphasis of the research was to identify the gaps and disconnects between different parts of an organisation in terms of understanding IT risk. The insight that this generated has allowed us to create a clearer picture of how organisations can identify their IT risks more accurately and therefore take positive steps to address them.

We specifically focused on answering three questions:

- Does the Board fully understand the impact that IT risk can have on the business and the need for assurance?
- Does Internal Audit provide assurance in the areas that the Board needs?
- Does Internal Audit have the credibility and capabilities to deliver assurance to the Board?

The research involved both quantitative electronic surveys from December 2006 and in-depth qualitative interviews with key personnel from April 2007. Views were obtained from senior management (including CFOs and CIOs) and from Heads of Internal Audit. Most organisations surveyed employ between 500 and 10,000 people and operate in a wide range of industries including the public sector. The findings were shared and ways forward discussed with a Head of Internal Audit focus group organised by the IIA in May 2007.

## Findings at a glance

87%

of organisations find it a significant challenge to keep abreast of IT change

98%

of organisations see IT as strategically important to the future success of the business

74%

of Internal Audit Heads would like to provide more assurance over IT risk at a strategic level

60%

of Boards see Internal Audit as able to discuss IT risks effectively

74%

of organisations now have IT related risk higher on the Board agenda

68%

of Internal Audit Heads believe the Board does not understand the IT risks they face

## Executive summary

The past two years have seen the re-emergence of large scale corporate investment into IT systems.

As a result of the transformation created by this investment, the Board is now looking for a greater level of comfort than ever before according to two thirds of our survey respondents. Supporting this key finding, we have found that:

- IT related risk is now higher on the Board's agenda than ever before, according to 74 per cent of senior managers surveyed.
- The risk of complex IT projects failing is likely to top the Board's list of IT worries.
- Keeping abreast of the pace of IT change, coupled with increased IT dependency is a significant challenge for 87 per cent of companies surveyed.

However, it is questionable whether Boards are adequately addressing their IT risk as they lack real understanding of their organisations' IT risks according to Heads of Internal Audit. The survey points to two possible reasons for this:

- Boards and Audit Committees may not have all the skills required to understand and challenge IT risk.
- The mechanisms for communicating IT risks to the Board may not be effective.

Internal Audit is well positioned to step up to these challenges and operate as prime navigator of the various sources of assurance, providing the Board with a complete picture of the risks and the comfort they get. But in order to step up, it will need to address the issues identified in our survey:

- Engaging with existing providers of IT assurance - IT quality assurance functions, compliance and other technical specialists - Internal Audit needs up to date technical knowledge to be able to challenge and assess findings.
- Meeting a demand for more strategic level assurance - for example looking upfront at the risks related to major IT transformation projects - providing the Board with early insight and clear choices for mitigation. This will require a greater level of credibility and enhanced communication skills within the business.
- Challenging the Board to help them fulfil their obligations around IT risk. This may include creating a clearer mandate for Internal Audit to inform the Board going forward.

In addition, Heads of Internal Audit may need to reassess their skills base and the way in which they engage with the business on IT.

“...and the non-execs really just want to know that everything is being controlled appropriately. They don't have the time to sit through a more extensive explanation and don't have the inherent practical experience of IT risk.”

Head of Internal Audit

# Survey findings

## Does the board fully understand the impact that IT risk can have on the business and the need for assurance?

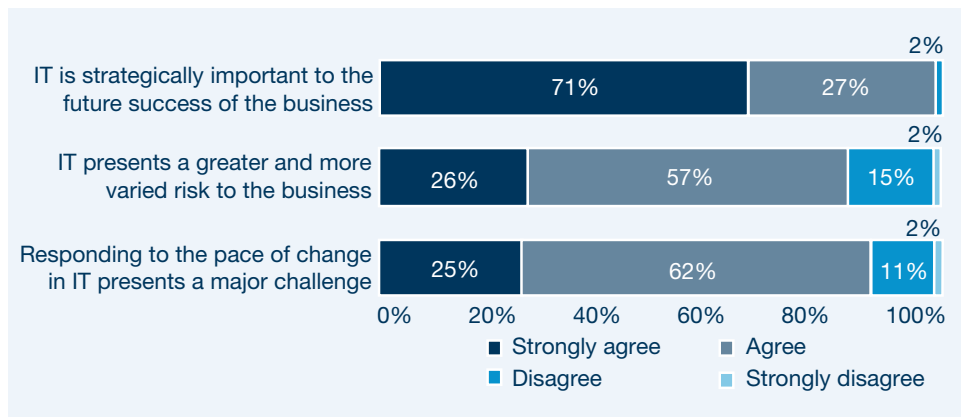
### Key findings

- 32% of Heads of Internal Audit believe the Board understands the IT risks they face
- Boards focus on potential IT benefits without corresponding risk
- IT professionals lack the ability to effectively communicate with the Board
- Board composition should be addressed to help them fulfil their obligations

A mutual understanding of IT risk is not always present, leading to the Board having an incomplete picture of the IT risks faced by the organisation.

The survey found a clear consensus that the Board is spending more time considering IT matters and that IT poses major challenges to businesses.

### Does the pace of change create a major challenge?



However, the results go on to paint a mixed picture of how the Board is perceived to understand the IT risks that it faces, with some gaps emerging. The majority (76 per cent) of senior management respondents believe that the Board sees IT risk as an increasingly important issue, and the same proportion feels that they understand the risks facing the organisation.

When we asked Heads of Internal Audit whether they believed the Board understood the IT risks that the organisation faces, a different picture emerged. Only 32 per cent said that they thought this was the case, in marked contrast to the senior management perception.

One Head of Internal Audit summarised the views of a number when he remarked: “The Board has less of an understanding. This is a constant challenge as meetings take place infrequently and the non-execs really just want to know that everything is being controlled appropriately. They don’t have the time to sit through a more extensive explanation and don’t have the inherent practical experience of IT risk.” Analysis by sector reveals differences in opinion, with retail, manufacturing and the public sector seeing less understanding of IT risk than their counterparts from other industries.

“Recognising the level of change that the business is going through and the dependency on reliable IT, the Board is actively seeking more assurance.”

Head of Internal Audit

Another Head of Internal Audit noted a tendency for the Board to focus on the business benefits that IT delivers rather than the potential risks to which it can give rise, saying: “IT is increasingly on the Board’s agenda – but the average Board member sees the potential for enablement much more than the risks. They don’t see the connection between the technical detail and the giant-killing issue.” Of course you would expect the Board to focus on the enablement but it is also important for them to understand the risks that need to be managed resulting from the use of IT. These risks should be considered at all levels because a small technical flaw can create a large operational issue for the organisation.

Assessing the extent of dependency on technology also helps organisations to determine the approach to managing technology risks and the likely need for assurance. Where there is a high dependency on IT, e.g. IT is strategic to the organisation (providing competitive advantage and there is high dependence on reliable IT), there will be a greater need for assurance. Where there is little dependency on IT, e.g. organisations that can quickly revert to manual procedures for major processing and there is little exposure of systems to customers or suppliers, there will be less need for assurance.

Over one-third of senior management respondents and almost half of Heads of Internal Audit believe that IT professionals lack the ability to communicate IT risk and potential business impact in a manner that the Board can readily understand.

Assessing risk is a team game, bringing together IT professionals who understand IT but may not fully understand the potential business impact that needs to be managed, and the business managers who lack a deep technical understanding of IT but could draw out the potential business implications. All have a role to play to ensure that the risks of new developments in IT and the resultant business implications are fully identified and understood by all parties.

The survey shows that this mutual understanding of risk is not always present, leading to the Board having an incomplete picture of the IT risks faced by the organisation. Facilitated discussions could aid people to come to a common understanding of the organisation’s dependency on IT, the resultant risks and the level of assurance needed. Internal Audit may be in a position to initiate and to facilitate such discussions – it already understands risk and communicates with the Board. The question is: what else does it need to do to play this role?

### Key questions for you to consider:

How do you validate that the right IT risks are appearing on the Board’s and Audit Committee’s agendas?

Is communication between the Board and IT effective enough to create the required awareness?

Is there a commonly held view on what level of assurance is required in your organisation?

“...it is not acceptable now for a Board member to say proudly ‘I am a luddite’. Five years ago they could have got away with that.”

Senior Executive

# Survey findings

## Does Internal Audit provide assurance in the areas that the Board needs?

## Where does Internal Audit focus its efforts?

### Key findings

- 75% believe the Board requires more comfort and assurance
- The top risk today is large projects with a significant IT component
- Internal Audit is failing to assure IT risk at both a strategic and detailed level – 74% of Internal Audit heads would like to provide more assurance
- Potential for new audit model between IT and Internal Audit

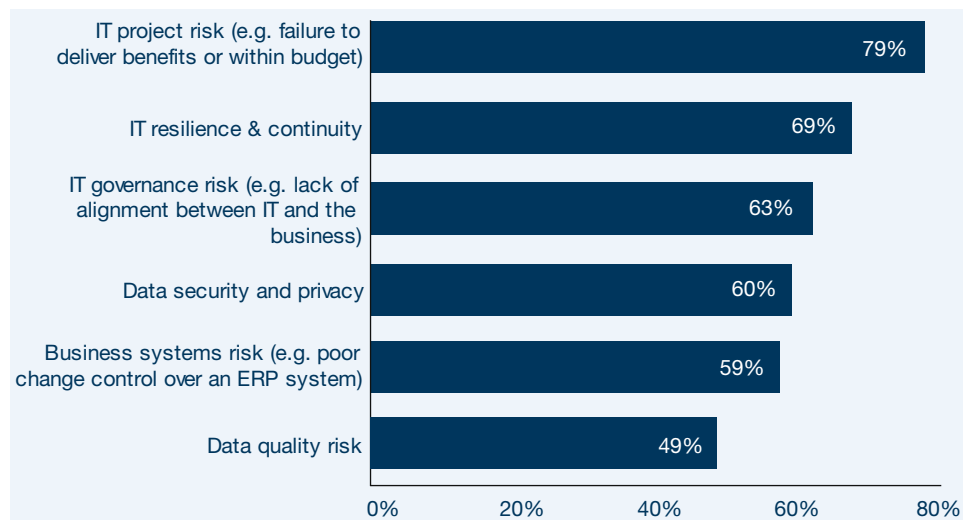
### The demand for assurance covering IT risks is not being met.

There is a demand for Internal Audit departments to focus more of their efforts on strategic and proactive reviews, for example, determining whether the right level of strategic input has been obtained to ensure the success of major IT transformation projects.

When we asked Heads of Internal Audit to indicate the amount of time that their departments currently spend on reviewing IT risks nearly 60 per cent confirmed that they spend less than 20 per cent of their time in this area. This level of focus is not meeting the demand for assurance covering IT risks. Around three-quarters of senior management and Heads of Internal Audit share the view that the Board is looking for more comfort and assurance than Internal Audit is currently providing.

In general, Heads of Internal Audit and senior management agree on the top six IT risks that organisations face, as illustrated below:

### Top six IT risks that organisations must deal with today, identified by both senior managers and Heads of Internal Audit



Senior management and Heads of Internal Audit agree that managing business projects with a large IT component (IT projects) is the top IT risk that organisations must deal with today. This is not surprising given levels of IT project activity across all industries. Organisations are rationalising or re-implementing ERPs and other major systems. These transformation projects increasingly include complex outsourcing and offshoring components and represent major business investments.

“The Board is looking for more assurance over strategic risk – we need to see IT as a component of this”

Head of Internal Audit

We asked Heads of Internal Audit and senior management to characterise the work that IT internal audit performed using the following definitions:

**Strategy/Governance** – Internal Audit has carried out work to review the strategic approach to a particular risk area or the manner in which it is governed.

**Processes and Procedures** – Internal Audit has reviewed the processes and procedures that have been put in place to manage a particular area of risk.

**Detail** – Internal Audit has conducted testing of a particular risk area at a detailed level, e.g. to assess the specific configuration of a system.

#### Perceived focus of IT audit work by Heads of Internal Audit

Head of Internal Audit View	Strategy/ Governance	Processes and procedures	Detail
IT project risk	●	●	●
IT resilience and continuity	●	●	●
IT governance risk	●	●	●
Data security and privacy	●	●	●
Business systems risk	●	●	●
Data quality risk	●	●	●
Emerging technology risk	●	●	●
IT asset management risk	●	●	●
IT outsourcing and offshoring risk	●	●	●
The impact of globalising IT operations	●	●	●
Compliance with regulation or external standards	●	●	●

- Selected by less than 20% or less of respondents
- Selected by more than 20% but less than 40% of respondents
- Selected by 40% or more of respondents

“The traditional IT auditor is more comfortable at the detailed level and, if left to their own devices, will test and test and test!”

Head of Internal Audit

Perceptions of the focus of Internal Audit's work show some interesting variations. Although at a high level 80 per cent of Heads of Internal Audit believe that they review IT risk from a strategic perspective, when asked to analyse work carried out on specific risks, they identified very few areas where they perform strategic level work. As the chart on the previous page shows, only IT governance is being addressed from a strategic perspective by a significant percentage.

Perhaps most surprising is that IT project risk – seen by both Internal Audit and senior management as the priority area – is receiving very little attention at any level from internal audit. It may be worth the Board confirming where it is getting comfort over this key risk, particularly at a strategic level.

When we asked senior management for its view, a far smaller proportion, 50 per cent, felt that internal audit reviewed IT risk from a strategic perspective. In addition, most believed more work was being carried out across all IT risk areas at the 'processes and procedures' level than reported by Heads of Internal Audit. These findings suggest that there is a misalignment between senior managers' perceptions of the assurance they receive versus that which internal audit provides. Again there is a case for ensuring that detailed and structured dialogue takes place that allows the gaps to be identified and addressed.

When asked, 74 per cent of Heads of Internal Audit said that they would like to provide more assurance around IT risk at a strategic or governance level than they currently do. Only 51 per cent felt that additional assurance at a detailed level was required. Internal Audit recognises the need to operate in a more pro-active way and at a strategic level. As one Head of Internal Audit observed: "The traditional IT auditor is more comfortable at the detailed level and, if left to their own devices, will test and test and test!" While the survey shows that there is a need to provide additional assurance at the detailed level, it may be worth thinking about the sources of this detailed assurance. For example, performing the detailed testing may not require audit knowledge, and this activity could therefore be performed by a technical specialist, and the results interpreted by the IT auditor, allowing the IT auditor to focus more of his/her efforts on matters of strategic importance.

Internal Audit departments that have not yet stepped up to the mark, need to consider how they will respond as senior management is keen for them to perform more strategic level reviews in order for them to deliver most value.

### Key questions for you to consider:

Are you assessing all your IT risks against the current market benchmark of IT risks on a regular basis?

Does the Board's need for assurance determine the effort dedicated to IT audit?

Are sufficient pro-active audits carried out at a strategic level to optimise the value provided to the business?

“...IT auditors need to have their ‘war medals’ as the business is far more likely to listen to them if they have actually done the things that they are recommending.”

Senior Executive

# Survey findings

## Does Internal Audit have the credibility and capabilities to deliver assurance to the Board?

### Key findings

- 40% of Boards do not see Internal Audit as able to discuss the business implications of IT risks
- A third believe IT Internal Audit lacks credibility within the business
- Audit ability and a related IT qualification are seen as desirable
- Internal Audit needs to develop a flexible delivery model to address pervasive change

### In-depth IT risk management, business skills and communication credentials are essential for success.

Well over one third of senior management respondents believe that internal audit departments, as they currently operate, lack the appropriate capabilities to provide the Board with the assurance over IT risks that is needed. Some Heads of Internal Audit agreed, suggesting that they are well aware of the challenges they face in providing effective assurance.

Heads of Internal Audit also acknowledge the need to work at a more strategic level within the organisation. Capabilities in terms of skills and technical knowledge are obviously important to make effective challenges to the status quo, but these need to be part of an overall 'package' that senior management and the Board finds convincing and credible.

While senior management might expect Internal Audit staff to have the appropriate credibility and related capabilities, only 60 per cent of respondents said that internal audit was able to discuss the business implications of IT risks effectively with the Board.

This gap is further demonstrated by the finding that almost a third of all senior manager respondents felt that IT internal auditors did not have credibility, such that their views were respected by the business. As one senior manager firmly in that camp commented: "If IT internal auditors are to move into that strategic space they need much more credibility and kudos than they currently have...IT auditors need to have their 'war medals' as the business is far more likely to listen to them if they have actually done the things that they are recommending."

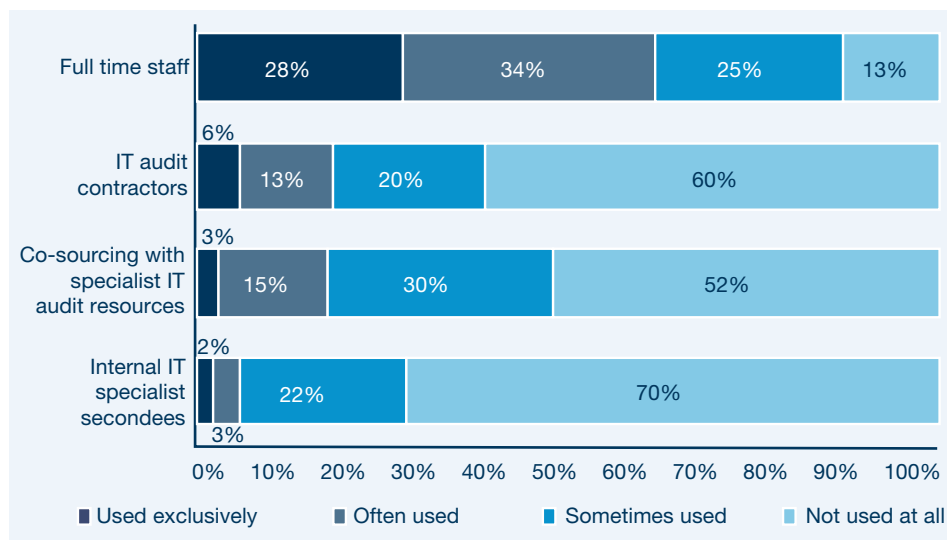
We asked Heads of Internal Audit how they resource IT audits (see chart on page 17) and 62 per cent responded that they rely on internal resources to fulfil IT internal audit obligations. A smaller percentage, between 15 and 18 per cent, use external contractors or some form of co-sourcing to help fill the gap.

Heads of Internal Audit were asked about their views on the effectiveness of a variety of methods to ensure that individuals have appropriate skills. An internal audit qualification and a specialist IT internal audit qualification were seen as desirable by over 75 per cent of respondents, with the specialist qualification considered to be the most effective.

“The most difficult thing about IT audit is that it’s three dimensional, you need a specialist for every single area and then someone putting everything together.”

Head of Internal Audit

### Where do you obtain the resources to provide assurance on IT risks?



An Internal Audit focus group held by the IIA to discuss the initial survey findings concluded that the breadth and depth of skills required to cover all current and emerging IT risks, made it both uneconomic and impractical to maintain all skills in-house. In terms of the skill requirement they confirmed that whilst both qualifications may be desirable, the most important requirements are that auditors know how to perform an audit. Looking forward, the group felt that Internal Audit's business and IT roles should integrate, with specific technical support provided by non-audit specialists as and when needed.

To achieve this integration, Internal Audit will need access to the right technically skilled people that can understand the IT risks and review how these are being managed. A holistic business perspective and good communication skills are needed to ensure the business implications are identified and communicated in a way that all parties understand. Internal audit will also need to develop a delivery model that is sufficiently flexible and responsive to deal with the pace of such pervasive change.

**Key questions for you to consider:**

Does the Internal Audit function have the right balance of business and technical skills needed to provide the assurance that the Board needs?

How do you fulfil this need in a sustainable manner?

# Appendix

## Mapping the spectrum of technology risks

The diagram below describes the 11 main areas of technology risk that PricewaterhouseCoopers

### IT governance

Managing the structure and framework within which IT operates can have a critical bearing on overall corporate performance. An MIT study found that businesses with below average performance in IT governance were 25 per cent less profitable than their peers whose performance was ranked as good or above.

### IT compliance

A number of different compliance standards have to be met, so a joined-up approach is essential. Otherwise, complexity can create inefficient overlapping controls or gaps that lead to non-compliance.

### Data security and privacy

Security of information is essential and breaches or leakages can be financially devastating and do significant damage to reputation.

### Business systems

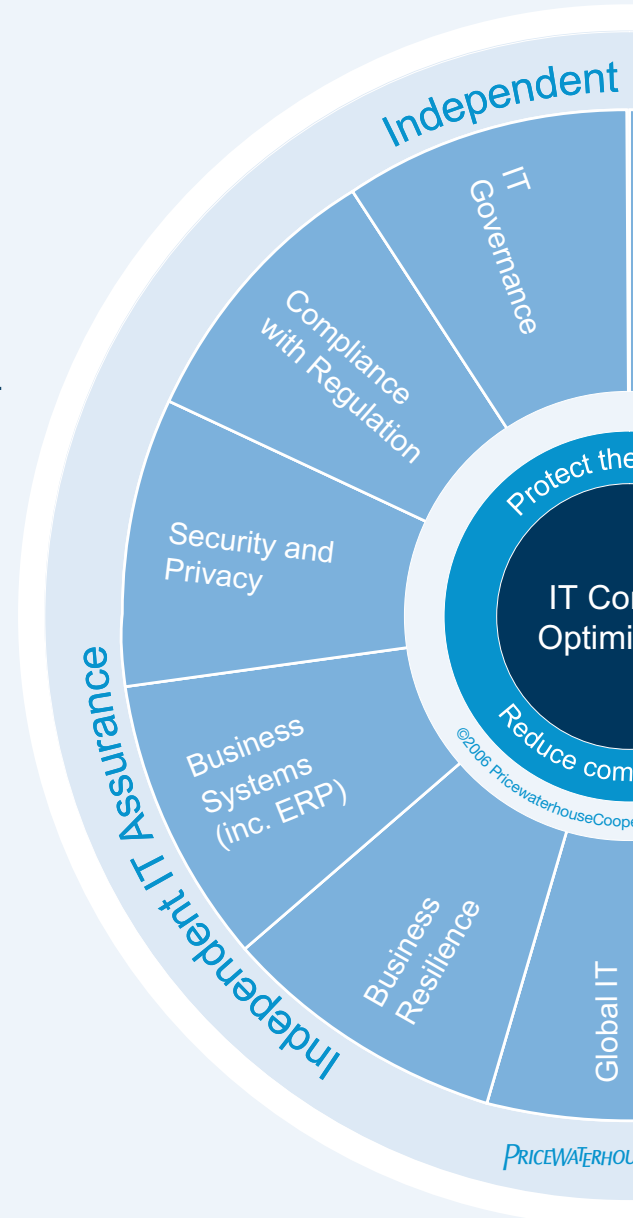
Business-as-usual updates to ERP systems can create significant control loopholes and security flaws as systems move away from integrated operation.

### IT resilience and continuity

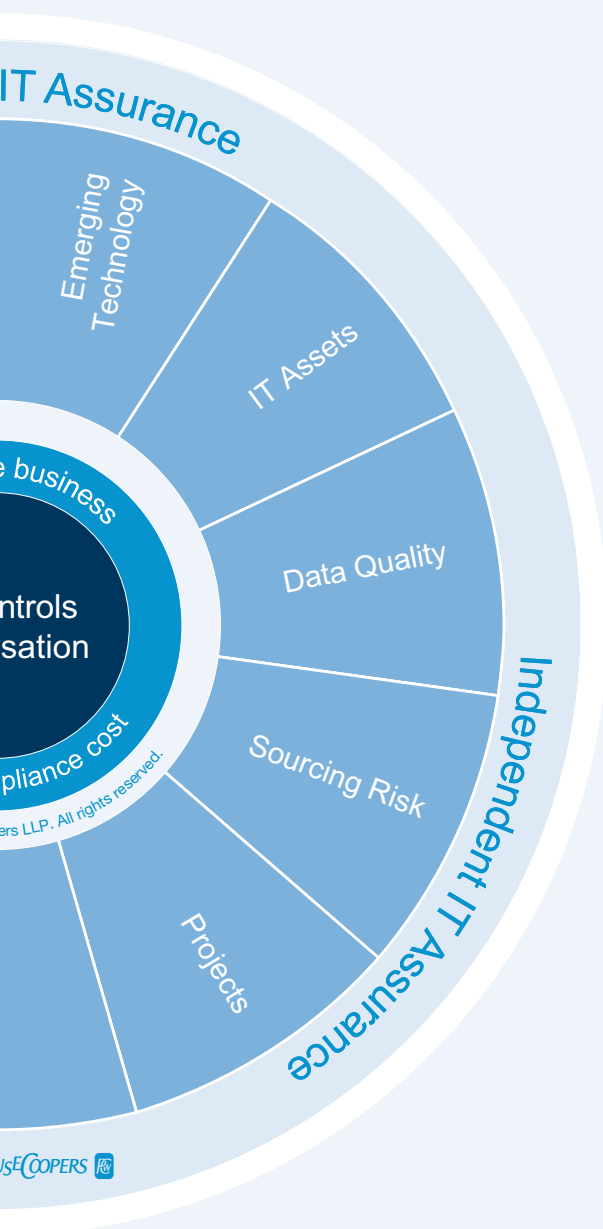
A loss of system availability can lead to higher costs, lost revenue and reputational damage. In extreme cases it can cause business failure. In fact, London Business School estimates that 57 per cent of all business disasters are IT-related.

### Global IT

Operating a global IT system creates additional complexity and risk. Differences in local approaches and attitudes can create global system vulnerabilities. Inadequate global support can lead to high levels of downtime and reduced effectiveness.



PricewaterhouseCoopers has identified through detailed discussions with many organisations



### Emerging technology

Responding quickly to adopt new technology can carry high risk exposure but adopting too late can cause loss of competitive advantage.

### IT asset management

An inaccurate or incomplete inventory of IT assets (both hardware and software) can create problems for security, impair effective investment and create exposure to financial and reputational damage arising from unlicensed software. For example, 90 per cent of all software licensing reviews carried out by PricewaterhouseCoopers have identified non-compliance.

### Data quality risk

Data is an organisation's lifeblood, allowing it to serve customers effectively and efficiently and gain competitive advantage. Poorly managed data, however, can have equally negative impacts, leading to inefficiencies, poor customer service and damage to reputation.

### IT sourcing

Many outsourcing arrangements fail to deliver the anticipated benefits, and are terminated early as a result. If not executed effectively outsourcing can result in unpredictable behaviour, political instability, poor processes and weakened security.

### IT projects

The volume, cost and complexity of IT projects is increasing. However, one quarter of all projects fail completely and half are delivered late or over budget.

“Internal Audit needs to be a strategic partner to the business – moving further up the value chain. They should have far more skin in the game.”

Senior Executive

## About the authors

### PricewaterhouseCoopers

The member firms of the PricewaterhouseCoopers network ([www.pwc.com](http://www.pwc.com)) provide industry-focused assurance, tax and advisory services to build public trust and enhance value for its clients and their stakeholders. More than 140,000 people in 149 countries share their thinking, experience and solutions to develop fresh perspectives and practical advice.

PricewaterhouseCoopers helps clients design and implement IT risk and control solutions that protect businesses and reduce compliance cost. We also provide independent IT assurance to business leaders and third parties.

For more information on this survey, to meet an Internal Audit specialist, or to enquire about latest market best practice, please call your PricewaterhouseCoopers contact or Grant Waterfall (on 020 7804 2040, email: [grant.waterfall@uk.pwc.com](mailto:grant.waterfall@uk.pwc.com)).

### Institute of Internal Auditors

The Institute of Internal Auditors represents, promotes and develops the professional practice of internal auditing, with 130,000 members in 165 countries worldwide, and 8,000 members in the UK and Ireland.

The Institute of Internal Auditors – UK and Ireland is the only professional body in the UK and Ireland solely dedicated to the profession of internal auditing. It is part of the global Institute of Internal Auditors, which sets the *International Standards for the Professional Practice of Internal Auditing*, and the *Code of Ethics*, which all members agree to follow.

For more information please visit the website at [www.iaa.org.uk](http://www.iaa.org.uk) or contact Justin Scott on 020 7498 0101

For more information visit  
[www.pwc.com/uk](http://www.pwc.com/uk)

[www.pwc.com/uk](http://www.pwc.com/uk)

© 2007 PricewaterhouseCoopers LLP. All rights reserved. "PricewaterhouseCoopers" refers to PricewaterhouseCoopers LLP (a limited liability partnership in the United Kingdom) or, as the context requires, the PricewaterhouseCoopers global network or other member firms of the network, each of which is a separate and independent legal entity.