

Insights on IT risk  
Business briefing  
June 2011

# The evolving IT risk landscape

The why and how of  
IT Risk Management today

A close-up photograph of vibrant green grass blades, each adorned with a clear, glistening water droplet. The blades are oriented vertically, creating a sense of height and freshness. The background is softly blurred, emphasizing the sharp details of the grass and the individual droplets.

# Contents

- IT risks in today's business risk landscape..... 1
- The IT Risk Universe ..... 5
- IT Risk Management ..... 10
- What organizations are doing ..... 14
- Taking action..... 16



# IT risks in today's business risk landscape

## The evolving IT risk landscape

The way in which companies interact with their employees, customers and other organizations is changing at an unprecedented rate. Mobile computing and new technologies such as cloud computing and social media are breaking down the walls of the conventional office and demolishing the old IT risk paradigm.

For example, an organization's hardware is now operated in low-cost countries, software is provided in the cloud and an organization's data is held all round the world. Corporate data is transmitted over the internet, communicated and discussed on social media channels, and can travel around the globe instantly through a variety of channels and platforms, captured on employees' smart phones, tablet computers and personal computers. These high-tech devices, through which data now flows freely, were once only the exclusive domain of the employers who provided them, but now they are mostly owned by employees. The result is personal information and important and proprietary company data often residing on the same low security devices.

Faced with these complex and ever-changing layers of risk in this new 'world without borders', IT risk programs must expand and adapt to meet these challenges.

IT risk has historically been dismissed as the sole responsibility of the IT department, and has not been considered a strategic business risk requiring an enterprise-wide focus. However, as the pervasive use of IT tools and technology continues to grow, impacting virtually every aspect of business function, it is becoming increasingly clear that managing IT risk is less about just IT, and more about managing risks for the whole business. Organizations must now include IT Risk Management (ITRM) within their overall enterprise-wide risk management approach.

Over the years, our annual *Global Information Security* surveys<sup>1</sup> have revealed that board members and audit committees are increasingly interested in information security. This is one of the most important measures an organization can take to potentially reduce IT risk. However not all IT risks are covered by information security; there is a lot more to do.

<sup>1</sup> For further detailed reading on information security, ask for a copy of *Borderless security: Ernst & Young's 2010 Global Information Security Survey*, or download from [www.ey.com](http://www.ey.com).

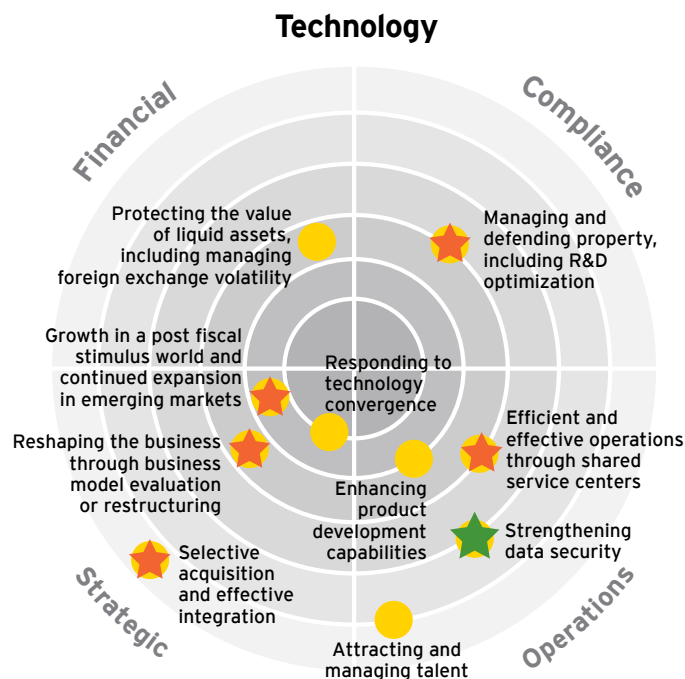
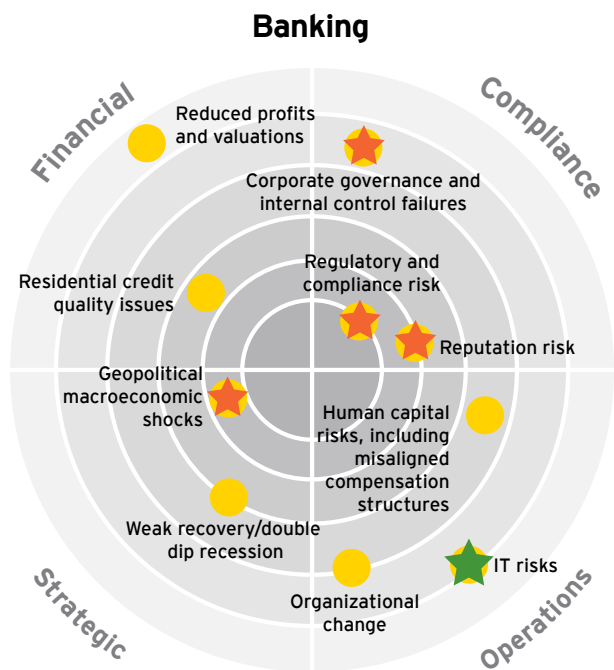


## IT risks are firmly linked to business risks

The Ernst & Young Business Risk Report 2010 looked at the top 10 risks across all business types, then by specific industry. By way of example, the 'risk radars' below show the top 10 risks for banks and for technology organizations.

These two sectors are heavy users of information technology. Risks related to IT are therefore listed as a separate category in their top 10 list. The banking sector has a generic 'IT risks' category (green star) while the technology sector focuses more specifically on 'data risks' (green star).

But there is more. In the graphs we have also highlighted (red star) those business risks in the top 10 that actually have a large IT component within them, containing a 'hidden' IT risk. Managing these business risks can only be achieved effectively when ITRM is an *integral part* of business risk management. Without ITRM an organization will fail to fully address these important business risks.



### Most of the business risks have a strong link to IT risks

- ▶ **Regulatory risk.** How will regulators respond to the increasing threat of IT risk?
- ▶ **Geopolitical shocks.** What is your exposure to these shocks? How responsive is your IT organization?
- ▶ **Reputation risk.** How would a cyber attack affect your reputation and brand?
- ▶ **Control failures.** Could gaps or weaknesses in IT controls and security be contributing factors?
- ▶ **IT risk.** How will you address the key risk areas of security, resilience and data leakage?

### Most of the business risks have a strong link to IT risks

- ▶ **Expansion in emerging markets.** Does increasing your company's footprint add to the challenge of business continuity?
- ▶ **Reshaping the business.** How much would your IT risk profile change?
- ▶ **Shared services centers.** Would this increase the risks to security and IT sourcing?
- ▶ **IP and data security.** Are you covered against data leakage, loss and rogue employees?
- ▶ **Selective acquisitions and effective integration.** How successful are your investments if you are not able to integrate the IT environment of an acquired company?

Source: The Ernst & Young Business Risk Report 2010. This item is available to download from [www.ey.com](http://www.ey.com).



To put it differently: ITRM is influenced by the same market forces as the other risks and is supportive to achieving the overall business objectives. It is within this business environment that organizations have to manage their 'IT Risk Universe'. This IT Risk Universe is provided in the framework below; it captures and highlights the 11 most significant risk categories (the eleventh category is 'strategy alignment' depicted in the center of the graph) which we will address in a later section in more detail. The risks within these categories will change over time depending on the IT megatrends organizations are facing. ITRM provides the overall risk and control framework that enables the most important control objectives for IT: effectiveness, efficiency, compliance, confidentiality, integrity, and availability.

## The growing importance of ITRM

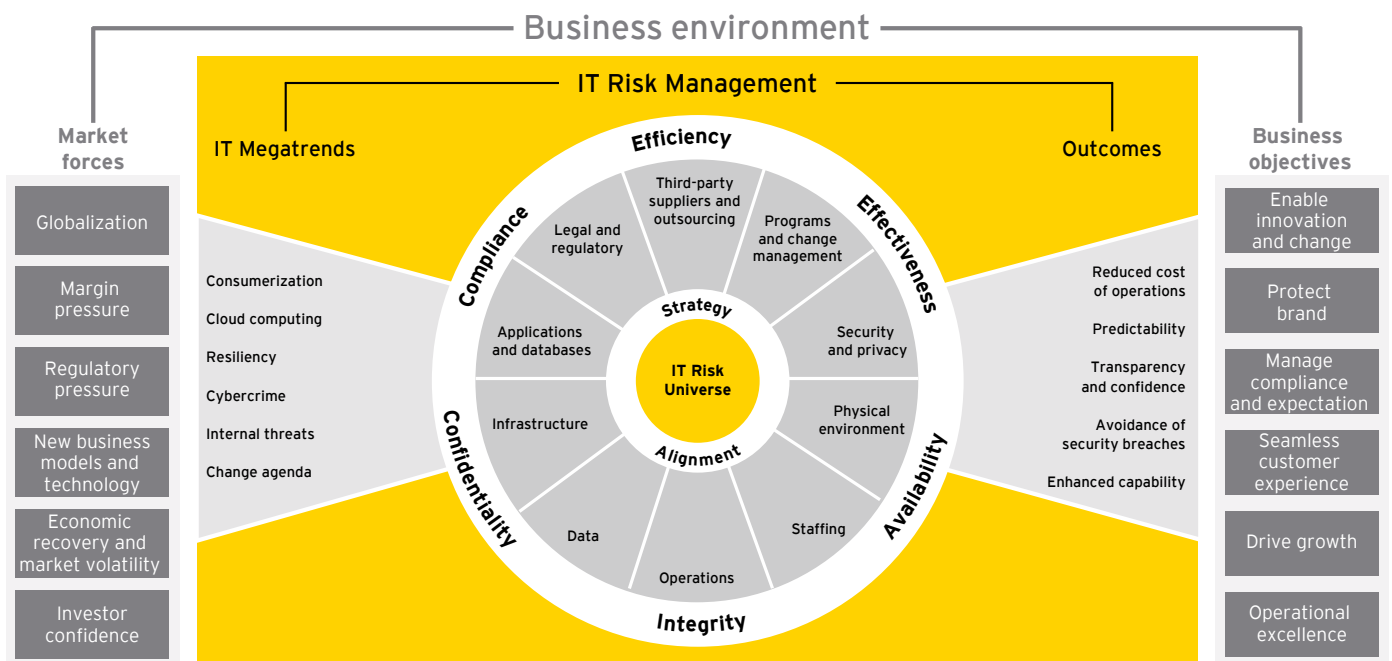
The IT risk paradigm has always been subject to changes, but the complexity and types of risk have expanded significantly over the years and will continue to do so. Evolving business models, increased regulation and deliberate acts of cybercrime all increase the exposure to risk and heighten the need to impose a new risk management regime. The graph on the next page shows how the risks have evolved over the years.

Some of the key risks to focus on and their implications for ITRM are:

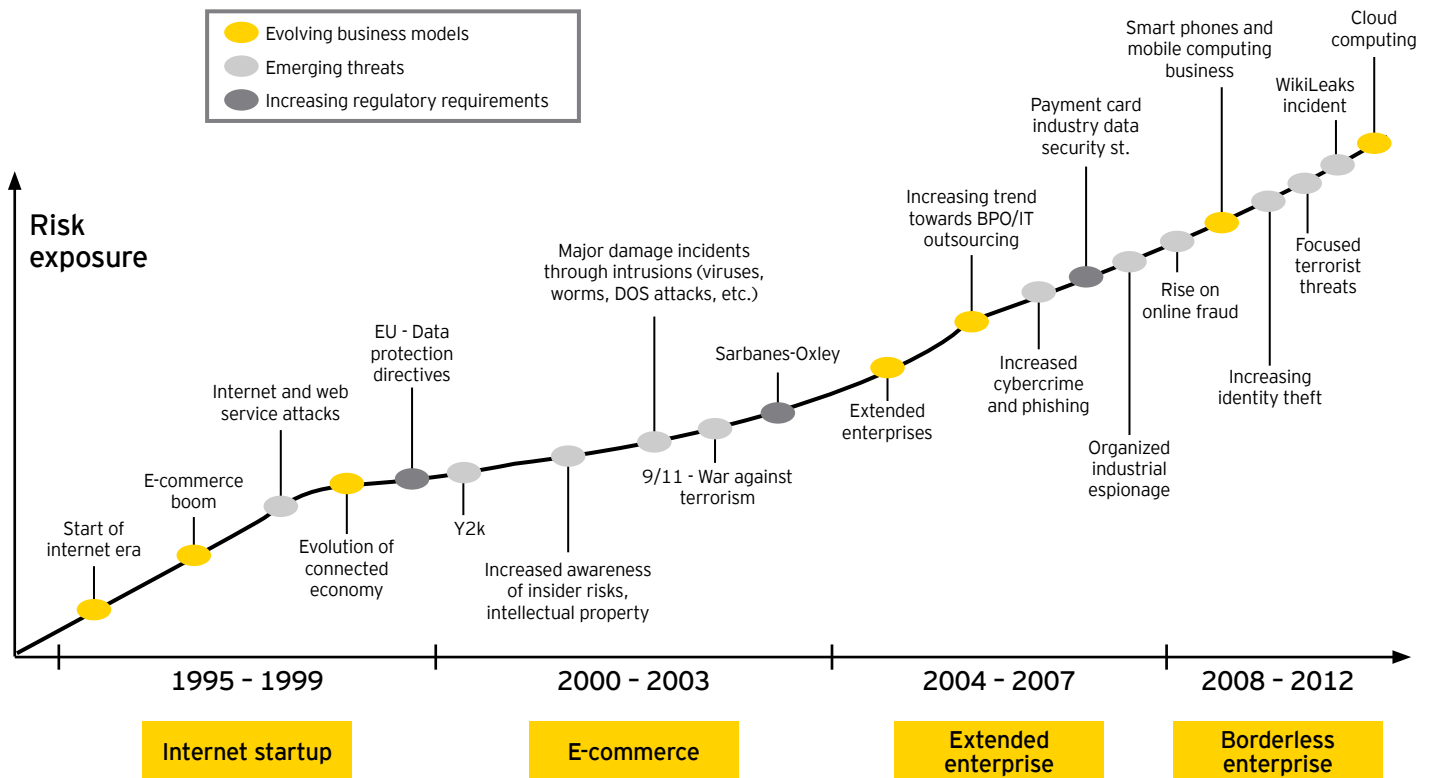
- ▶ Trends like business process outsourcing (BPO), cloud computing and IT outsourcing are all creating greater dependency on third parties. Therefore managing business continuity – and ensuring the availability of IT facilities – has additional external dimensions and complexities.
- ▶ Events like the WikiLeaks incidents, identity theft and mobile computing are forcing companies to focus more on data leakage risks.
- ▶ EU data protection directives are helping companies take action against increased cybercrime, phishing and online fraud.

It is clear that – with the exception of concerns about issues related to the start of the new millennium – IT risks are only increasing. The breadth and depth of the risks and the need for effective counter measures is expanding rapidly, and will likely continue to accelerate. Many businesses are recognizing this: in our recent IT Risk Agenda Survey<sup>2</sup>, two-thirds agreed that managing IT risk has become more challenging over the past few years.

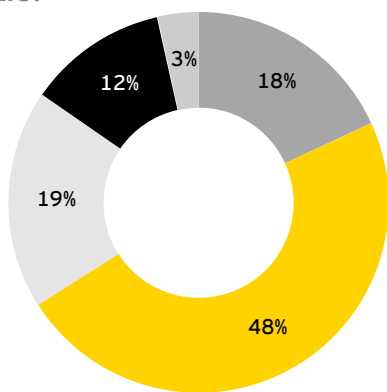
## The business environment and ITRM



<sup>2</sup> See 'About our Survey' at the end of this report.



**Has managing IT risk become more challenging over the past years?**



- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree

The growth of technologies such as mobile computing, cloud computing and virtualization, and the rapid adoption of social media platforms and online commerce/payments shows little sign of slowing. Newer technologies will continue to be created, each posing their own new set of risks and challenges, the nature of which cannot be easily predicted. Some organizations have embraced the new technology and harnessed it to help grow their businesses. (For example, the new consumer product and services discount website 'Groupon' needed only three years to achieve US\$ 1 bn in revenue). For these fast-moving companies, reliance on effective ITRM is considerable. They understand that an IT risk incident imperiling data and undermining consumer confidence could threaten their very existence.

Cybercrime is a highly unpredictable risk and has inevitably drawn increasing governmental regulation and oversight scrutiny. The EU data protection directives, Sarbanes-Oxley and the Payment Card Industry data security standards have therefore also become significant drivers of investments in ITRM-related processes and procedures.



# The IT Risk Universe

In order to effectively manage IT risks, organizations need to get a broad and complete view of the entire IT risk landscape. We have developed a framework to provide such a view, called the IT Risk Universe. This holistic perspective provides companies with a starting point to help identify and manage current IT risks and challenges, and those that may evolve over time.

The IT Risk Universe highlights the need for an aligned strategy to manage the 11 broad risk categories. These categories are relatively stable but the risks within these categories will vary company by company and will evolve over time.





## How different business environments impact IT Risk Universe

With IT risks so closely bound to business-wide risks, board members should be asking critical questions about the effectiveness of managing IT risks. To help identify these important and revealing questions, board members don't need to have detailed IT knowledge.

They just need to be clear on two things: how much their company relies on cost-effective, uninterrupted and secure IT systems (defensive IT), and how much their company relies on achieving competitive advantage through IT (offensive IT) or both. This understanding will help drive the questions they need to ask.

Companies can plot themselves on this "IT Strategic Impact Grid" to help gain perspective on their IT priorities, How 'business critical' their day-to-day operational functions are, and whether IT requires greater innovation and investment.

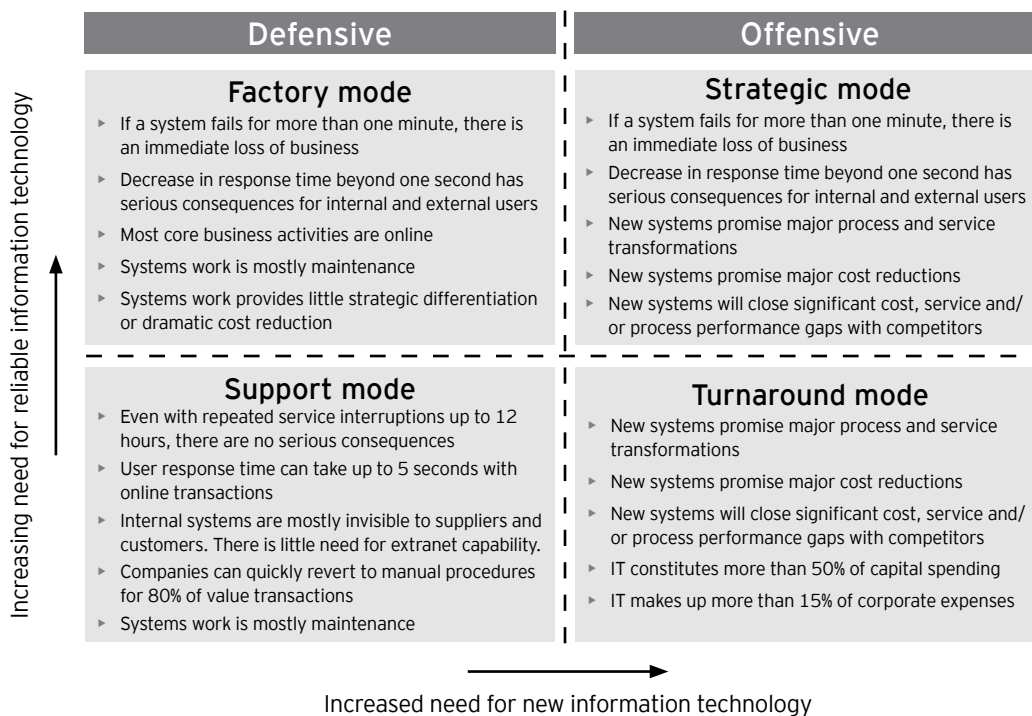
Once an organization is aware of the mode they are in, they can focus on what is important for their specific circumstances and implement customized governance and controls as necessary.

Note that large organizations are almost never in a single mode. They can be in several modes of the quadrant at the same time, depending on the part of the organization that is examined and the core applications in use in this part of the organization.

For example: organizations (or parts thereof) in 'Factory' or 'Strategic' mode (scoring highly on the vertical axis) should focus on business continuity measures to prevent operational disruptions. For these types of organization, information security and reliability should be on the agenda of boardroom discussions. The board should, for example, ensure that management monitors the organization's networks on security breaches and that business continuity and disaster recovery plans are in place and effective.

Organizations (or parts thereof) in 'Turnaround' or 'Strategic' mode (scoring highly on the horizontal axis), should focus more on managing IT investments in innovation, and maintaining an overview of the continuously changing IT landscape. The risk management activities would typically focus on the mitigation of risk associated with IT projects, programs and change management initiatives. Typical control activities could, for example, focus on assurance of strategic IT projects, the maturity of configuration and change control processes, and control over the enterprise architecture.

### IT strategic impact grid



Source: "Information Technology and the board of directors," Nolan & McFarlan, Harvard Business Review, October 2005.



## IT Megatrends help identify the IT risks that matter

To help best appreciate the IT Risk Universe and to build an ITRM approach, it is helpful to understand that IT risks are impacted heavily by a number of significant trends – so-called “megatrends”.

Each of these megatrends brings with them great opportunities as well as new and complex challenges. Each of these megatrends links to the IT Risk Universe in several ways, as shown in the table below:

Megatrends	Business benefit	Business/IT risks	Categories of IT Risk Universe affected
<b>Emerging consumerization</b>	<ul style="list-style-type: none"> <li>▶ <i>Mobile computing:</i> Anytime and anywhere connectivity/ high volume portable data storage capability</li> <li>▶ <i>Social media:</i> New and advanced information sharing capabilities such as crowdsourcing.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Increased vulnerability due to anytime, anywhere accessibility</li> <li>▶ Risk of unintended sharing, amplification of casual remarks, and disclosure of personal and company data. The availability of this data on the web facilitates cyber attacks</li> <li>▶ Employees may violate company policies in terms of data leakage</li> </ul>	<ul style="list-style-type: none"> <li>▶ Security and privacy</li> <li>▶ Data</li> <li>▶ Legal and regulatory</li> <li>▶ Infrastructure</li> </ul>
<b>The rise of cloud computing</b>	<ul style="list-style-type: none"> <li>▶ Lower total cost of ownership</li> <li>▶ Focus on core activities and reduction of effort spent on managing IT infrastructure and applications</li> <li>▶ Contribute to reduction of global carbon footprint</li> </ul>	<ul style="list-style-type: none"> <li>▶ Lack of governance and oversight over IT infrastructure, applications and databases</li> <li>▶ Vendor lock-in</li> <li>▶ Privacy and security</li> <li>▶ Availability of IT to be impacted by the use of the cloud</li> <li>▶ Increased risk to regulatory non-compliance (SOX, PCI etc.). The cloud also brings about challenges in auditing compliance.</li> <li>▶ The cloud may impact the agility of IT and organizations; the platform dictated by the provider may not align with software development and strategic needs of the user</li> </ul>	<ul style="list-style-type: none"> <li>▶ Security and privacy</li> <li>▶ Data</li> <li>▶ Third-party suppliers and outsourcing</li> <li>▶ Applications and databases</li> <li>▶ Infrastructure</li> <li>▶ Legal and regulatory</li> </ul>
<b>The increased importance of business continuity</b>	<ul style="list-style-type: none"> <li>▶ 24/7/365 availability of IT systems to enable continuous consumer support, operations, e-commerce, etc.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Failure of the business continuity and disaster recovery plans causing financial or reputational loss</li> </ul>	<ul style="list-style-type: none"> <li>▶ Infrastructure</li> <li>▶ Applications and databases</li> <li>▶ Staffing</li> <li>▶ Operations</li> <li>▶ Physical environment</li> </ul>
<b>Enhanced persistence of cybercrime</b>	<ul style="list-style-type: none"> <li>▶ N/A</li> </ul>	<ul style="list-style-type: none"> <li>▶ Spread of malicious code in company systems causing system outages</li> <li>▶ The risk of theft of personal, financial, and health information</li> <li>▶ Loss of confidential data due to external vulnerabilities</li> <li>▶ Financial loss due to unauthorized wire transfers</li> </ul>	<ul style="list-style-type: none"> <li>▶ Security and privacy</li> <li>▶ Data</li> </ul>
<b>Increased exposure to internal threats</b>	<ul style="list-style-type: none"> <li>▶ N/A</li> </ul>	<ul style="list-style-type: none"> <li>▶ Assigning access rights that are beyond what is required for the role by employees or contractors</li> <li>▶ Failure to remove access rights for employees or contractors on leaving the organization</li> </ul>	<ul style="list-style-type: none"> <li>▶ Data</li> <li>▶ Applications and databases</li> </ul>
<b>The accelerating change agenda</b>	<ul style="list-style-type: none"> <li>▶ Fast adoption of new business models or reducing costs provides organizations with competitive advantage</li> </ul>	<ul style="list-style-type: none"> <li>▶ Failure to deliver IT projects and programs within budget, timing, quality and scope causing value leakage</li> </ul>	<ul style="list-style-type: none"> <li>▶ Programs and change management</li> </ul>



**1. Emerging consumerization:** This is when new information technology emerges first in the consumer market and then spreads into business organizations. This results in the convergence of the IT and consumer electronics industries, and a shift in IT innovation from large businesses to the home. Mobile computing and social media are examples of consumerization that are increasingly being adopted by a wide audience and across many demographic groups. They are examples of how technology is providing the user with great convenience such as anytime and anywhere access to information (mobile computing), enhanced information sharing capabilities (social networking) and high volume data storage portability (mobile computing). Consumerization also brings about new risks related to accessibility through mobile computing or the unintended disclosure of personal or company data through social media.

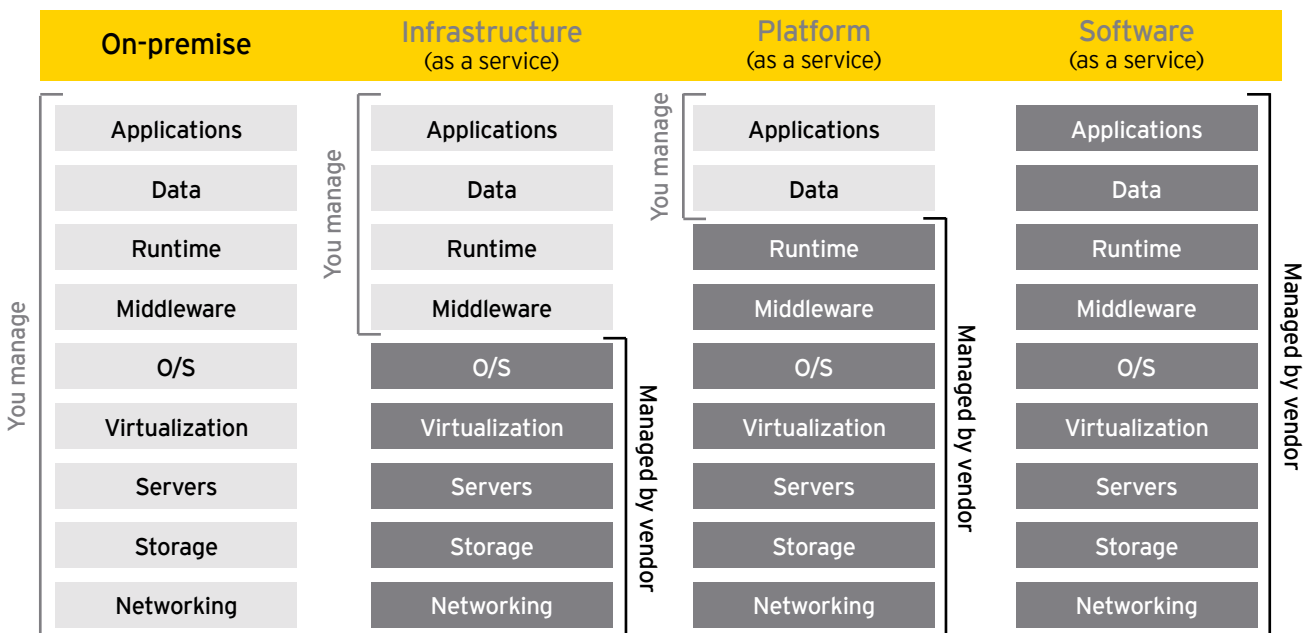
**2. The rise of cloud computing:** This is a means of using the internet to access data, using a third party's software running on yet another party's hardware, potentially in yet another party's data center. In this example, that data center is usually operated by a cloud service provider that offers a pay-as-you-go service. As shown in the diagram below, this is offered in several common market services including IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service).

Companies are increasingly using the "cloud" to support all of (or portions of) their systems landscape. Various surveys on internet usage show that more than 50% of large corporations now source

at least parts of their IT in the cloud. The benefits to using cloud computing include a reduction of the total cost of ownership, and it allows organizations to focus on their core business since it reduces the overall effort to managing infrastructure operations. On top of these benefits, the increased adoption of the cloud will reduce our overall ecological footprint since it allows for more effective utilization of IT assets. The cloud also brings several new risks and challenges that need to be managed, such as the ownership of data, availability risks, and challenges in auditing regulatory compliance.

**3. Resiliency:** As companies grow in complexity and interconnectivity, the impact of non-availability of any of the IT resources has magnified. In the current world of the "borderless enterprise," there is a visibly cascading impact of the inability of any part of the organizational value chain to deliver on its commitments. In addition, many businesses are increasingly dependent on their IT systems for 24-hour availability for their sales and customer support, or other core company operations. Although the importance of business continuity and disaster recovery is recognized by many companies, others still struggle. Many companies don't have business continuity plans, and those that do rarely test them. Business continuity has a more prominent position in the IT Risk Universe than ever before. This is evidenced by the results of the *Ernst & Young Global Information Security Survey 2010* which showed that the availability of IT resources is identified as the number one risk.

## Data center services





**4. Enhanced persistence of cybercrime:** Companies have increasingly been victims of cybercrime. FBI statistics show that the cybercrime rates in 2009 and 2010 were higher than ever before and 20% up on 2008. Research by the UK government (Office of Cyber Security & Information Assurance) has shown that the overall cost to the UK economy from cybercrime is approximately £27bn per year. The study shows that the majority (£21bn) of the loss is being born by UK businesses and that these losses are attributed to leakage of vital company data since 'espionage' and 'IP theft' are the two largest sources of economic loss in the UK. Cybercrime was initially the work of individuals that undertook hacking activities such as identity theft for their own personal financial gain. More recently, cybercrime has become perpetrated by more organized groups working in concert, leveraging more resources, skills and reach. Advanced Persistent Threats (APTs) are a growing issue. The nature of these activities is that they are not focused on short term gains; the goal is to stay uncovered and to collect as much vital company information as possible (IP, rates, proposals, new product design, strategic plans, etc). Traditional information security measures are relatively ineffective against these APTs and this has forced organizations to take additional measures against external threats.

**5. Increased exposure to internal threats:** The recent exposure of Wikileaks-related incidents have shown that internal security is at least as important as external threats. In one incident a disgruntled (ex)-employee of a Swiss bank handed over the bank account data of more than 2,000 prominent individuals to Wikileaks, potentially exposing tax evasion. This incident emphasizes once more that employees with access to critical, restricted information can put organizations at risk by disclosing the information to the public. This risk has recently been fueled by a rise in rogue or disgruntled employee behavior as a consequence of the financial

crisis, or from a sense of acting in the public interest. In practice, many firms are struggling with the management of providing the right access to information to the right people in their organizations. Experience tells us that: (1) companies are not able to articulate what their most valuable and important data elements are, (2) where these data elements are and (3) where these data elements are sent to.

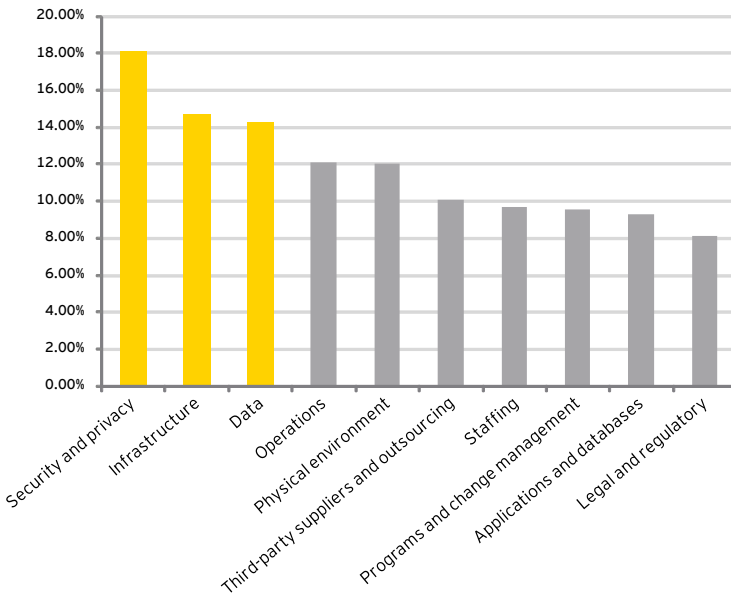
**6. The accelerating change agenda:** Change remains a "constant" in IT. Companies have historically put much effort in building and professionalizing an ERP landscape to support their core processes. Nowadays, the focus seems to shift to the surrounding suite of the ERP core such as Governance Risk & Compliance (GRC) and business intelligence. In addition, the financial crisis has put a break on innovation with many organizations due to budget cuts. They have therefore ceased to invest in strategic change in the past years leading to a significant installed base of IT legacy. For these two reasons, IT projects and programs remain top IT priorities.

The statistics on IT projects and programs, however, are not encouraging: according to the regular reports published by Standish, approximately 2 out of 3 projects are classified as 'not successful' meaning that they are either over budget, too late or not delivering the anticipated benefits. The low success rate causes a severe value leakage in IT organizations since they receive less 'bang for the buck' invested in IT as anticipated. In order to increase the success rate in IT projects and programs, organizations may take additional measures such as implementing Quality Assurance programs on major strategic programs.

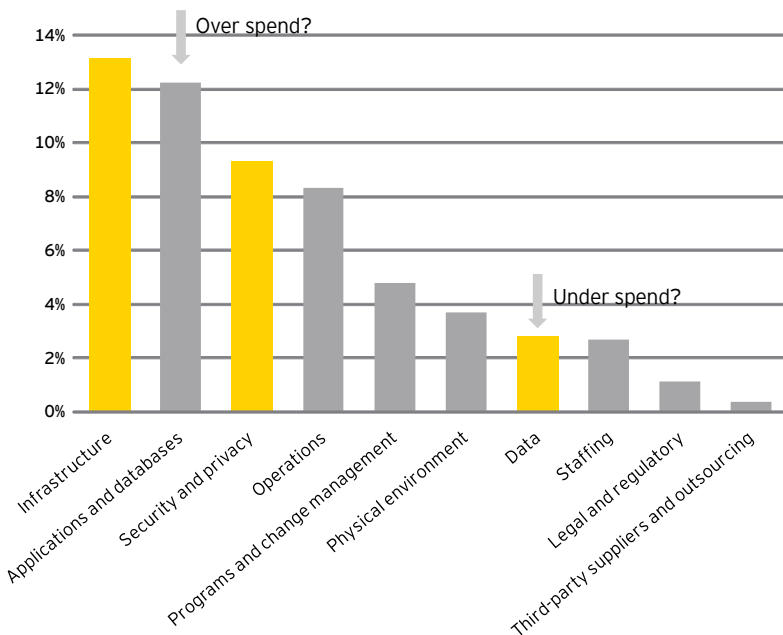
For further reading on these trends and other related topics, refer to our report, *Innovating for growth: IT's role in the new global economy* (available from [www.ey.com](http://www.ey.com)). This report discusses these trends and other related topics in more detail.

# IT Risk Management

In the following areas of IT risk, did your organization experience a negative incident or event in the past 12 months (response rate 'yes')?



For each of the following areas of IT risk, does your organization plan to spend more, less or the same over the next 12 months (in comparison with the previous 12 months) to mitigate the associated risks? (Y-axis scale: % participants responding 'more' - % participants responding 'less')



## Today's megatrends in IT

To address the evolving trends in IT risk, and any critical categories within the IT Risk Universe, many organizations may need to do some significant re-evaluation or readjustment of their ITRM approach. It should take into account not just the current state, but also factor in the future business response to the megatrends.

In our survey, we asked executives in which categories of the IT Risk Universe they had experienced the most negative IT-related incidents. Our results show that the three most commonly experienced incidents were in the categories of (1) security and privacy, (2) infrastructure and (3) data. It is not a surprise that all three categories also relate to most of the IT megatrends.

We then also asked the participating executives if they planned to spend more or less on the different IT Risk Universe categories. Their response (see below) shows that:

- ▶ security and privacy and infrastructure are recognized as high risk areas and organizations are planning to spend more to mitigate these risks
- ▶ although applications and databases are not immediately a high risk category, organizations plan to spend more (with the potential risk of overspending)
- ▶ the risks around data are not yet very high on the corporate agenda (implying a potential risk of underspending).



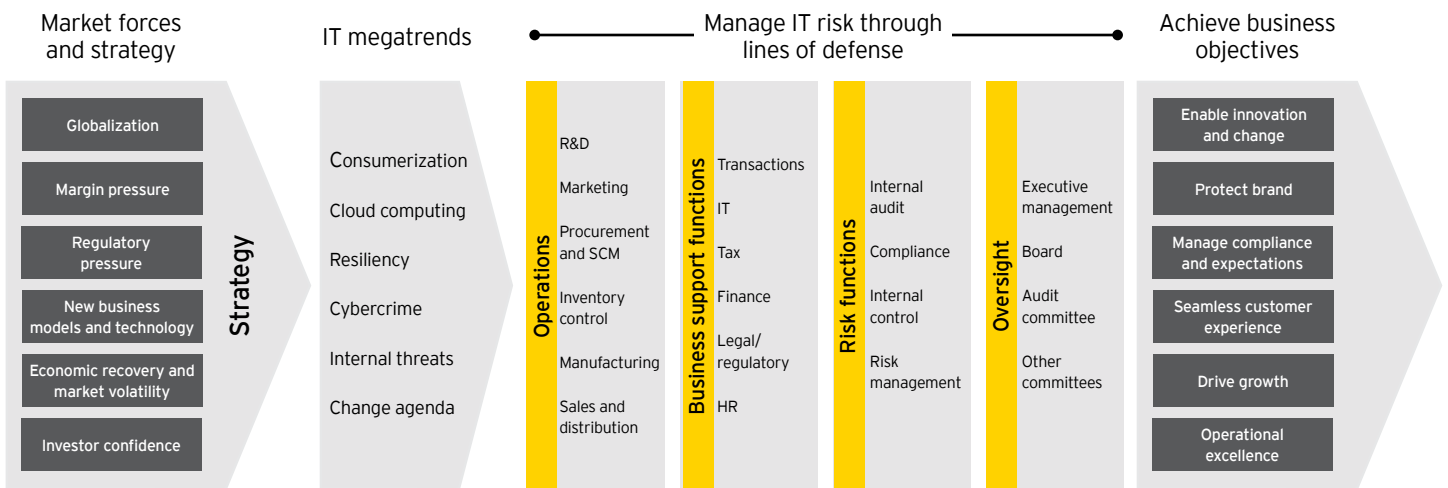
## Taking responsibility for managing IT risk

A key challenge for large companies is how to effectively embed ITRM efforts across the enterprise. It is not possible for any one single control, function or organizational layer to mitigate today's complex IT risks. Risks need to be coordinated along the several lines of defense each organization has. Companies therefore need to implement controls across these various lines of defense to bring the inherent IT risks back to a level that aligns with the company's strategic risk appetite. The overall effectiveness of ITRM is thereby determined by how well organizations are able to build effective controls across these lines of defense and across all functions and stakeholders.

## Creating a pro-active ITRM framework

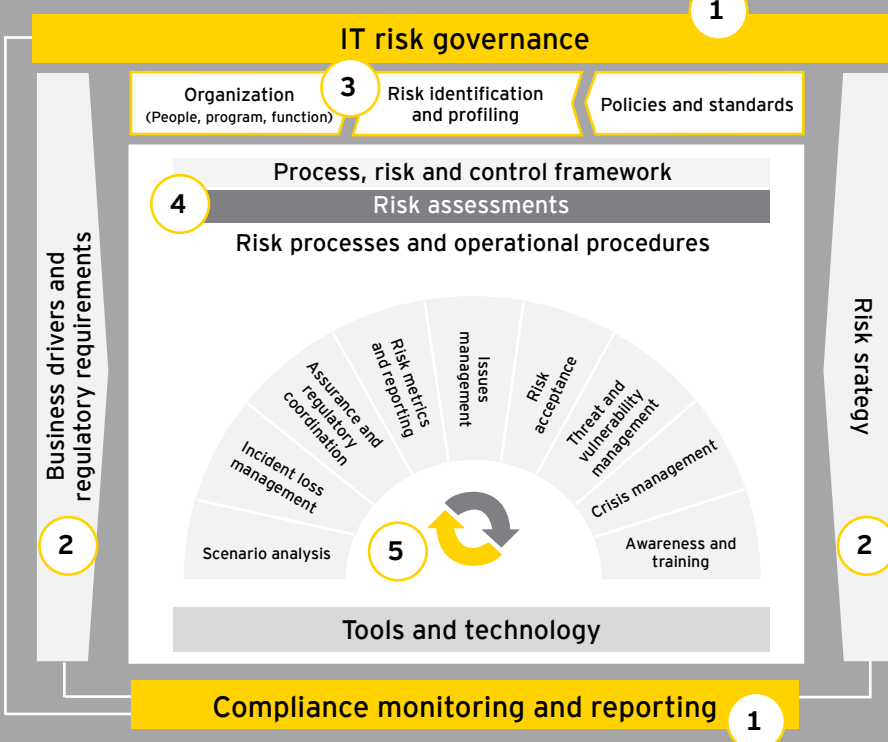
The first step in building an effective and proactive ITRM program is to identify its core components. This is where organizations can leverage their existing risk management framework to ensure consistent coordination, collaboration, risk coverage and risk management across the enterprise. The graphic on the next page shows a detailed ITRM framework and addresses the key components from the top down.

## Different functions involved in managing risk: lines of defense



The ITRM activities and processes (e.g., risk assessment, issue management, crisis management) are performed by many different functions in every organization within the several lines of defense. Insight into the processes and activities is provided in the subsequent sections of this article.

# IT Risk Management program



# Outcomes

- Risk**
- ▶ A risk conscious culture established at the top and cascaded throughout the organization
  - ▶ Streamlined risk and control operations
  - ▶ Reliable insights in risks supporting decisions and enabling performance
- Cost**
- ▶ Rationalization or reduction of risk overlaps and redundancies
  - ▶ A focused effort on the risks that really matter versus the low risk areas
- Value**
- ▶ Enabling confidence to take risk as opposed to avoid risk
  - ▶ The risk function provides process improvement suggestions

## 1 IT risk governance & compliance monitoring and reporting.

Ownership, accountability, and oversight are the cornerstones of any risk management program. The risk governance component of the ITRM program should have a strong leader, an executive who can juggle strategic and tactical enterprise initiatives across diverse and distributed IT environments. The overall governance of an ITRM program is supported by the IT risk dashboard to enable ongoing (compliance) monitoring and reporting on program effectiveness and risk posture.

This is where organizations put in place their processes to assess compliance with policies, standards, procedures, and regulatory requirements. Monitoring and reporting capabilities are designed to provide management with organizational views and trend analyses for risks, control issues, and vulnerabilities.

## 2 Business drivers, regulatory requirements and (IT) risk strategy.

Most organizations do not spend enough time clearly defining those critical business issues or business drivers that create the need for an ITRM program. These drivers must be aligned with business objectives, regulatory requirements, and board of directors and executive management directives. Without such alignment, there is the potential for confusion in coordinating various agendas and communicating the overall enterprise risk vision. This vision should encompass risk-tolerance guidance, risk processes, expectations for the risk management function, and the integration of risk processes such as IT security into standard IT operations.

**3 Organization/Risk identification and profiling/Policies and standards.** ITRM should be supported by a proper definition of roles and responsibilities. In addition, the ITRM program must define policies, standards, and guidelines that are fair to all stakeholders, and that provide an effective management of the operational procedures themselves. This includes specifying who has ownership and accountability for defining the organization's IT risk procedures, and for providing the oversight and guidance for formulating them.

Since organizations operate in a constantly changing risk environment, the organization needs to define a consistent process for identifying and classifying risk. This includes defining a taxonomy for risks and internal controls, risk ratings, prioritization of gaps, and parameters for the frequency and rigor of IT risk and internal controls assessments. Risk profiling reveals the gaps in a company's processes for managing its risks across the spectrum of potential exposures – legal, political, economic, social, technological, environmental, reputational, cultural, and marketing. Risk prioritization indicates the relative importance of the risk, including the likelihood of the threat, the degree of vulnerability and the potential business impact.

**4 Process, risk and control framework.** The organization should have a framework incorporating an IT process, risk and control framework (a library) with associations to regulatory, leading practices and internal requirements. In addition, the organization needs to design methodologies and procedures to enable a sustainable and repeatable assessment of IT risk in support of ITRM goals.

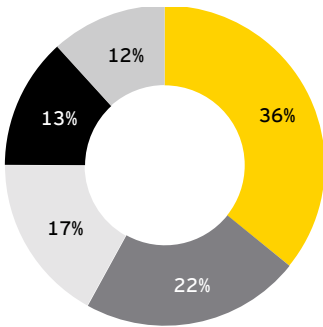
**5 Risk processes and operational procedures.** Processes and operational procedures represent the heart of the execution phase of an ITRM program and should be directly linked to the chosen risk management standard. This is the critical point for ITRM. Core components should include:

- ▶ **Scenario analysis** for disasters and events
- ▶ **Incident loss management** to capture events and estimate their financial impact
- ▶ **Assurance and regulatory coordination** for the risk management processes to support the continuous enhancement of IT-oriented risk data and processes
- ▶ **Risk metrics and reporting** to achieve continuous insight in risk exposure
- ▶ **Issues management** to operationalize the handling of issues
- ▶ **Risk acceptance** for the residual risks by management
- ▶ **Threat and vulnerability management**
- ▶ **Crisis management** during disasters or major events
- ▶ **Awareness and training** to increase the capabilities to achieve operational excellence in ITRM



# What organizations are doing

Which of the following best describes the ITRM program in your organization?



- **Level 5**  
The program has been well-established for several years
- **Level 4**  
We introduced a program within the past three years
- **Level 3**  
We are in the process of implementing a program
- **Level 2**  
We are currently evaluating options for a program
- **Level 1**  
We are not considering a program

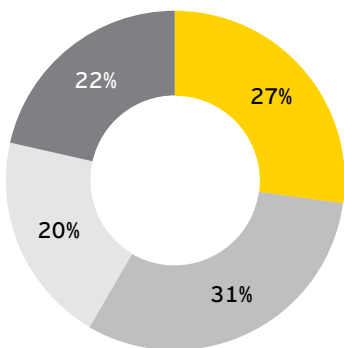
## Adoption of ITRM

In the IT Risk Agenda Survey we investigated the degree of adoption of ITRM. We found that over one third of the organizations had a well-established program and that almost a quarter had only recently implemented an ITRM program. Another 30% were either implementing a program or considering a program. Further in-depth analysis of these results also shows that there is also a correlation between the size of business and the adoption percentage: large companies (700 employees or more) are significantly more likely to have an established ITRM program in place than companies with fewer employees.

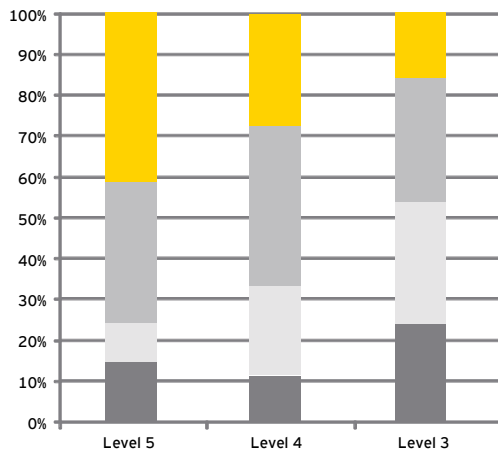
## The use of tools

Many software vendors offer risk management or GRC (Governance Risk & Compliance) services. These tools often link their business requirements with a reporting tool that can aggregate various risk elements and information in order to obtain an enterprise-wide view of IT risk. We asked the participants in the IT Risk Agenda Survey if they used such supporting tools. We found that the more mature the ITRM program is within an organization, the more likely it is that the organization uses tools. In our view an organization should seriously consider the adoption of appropriate tools - our survey suggests that the use of tools may be a key component in the achievement of a mature ITRM program.

Does your organization use any tools or software applications to support ITRM (e.g., GRC tools)?



- Yes - we rely upon these to support our IT risk management efforts
- Yes, but we use these on a limited basis only
- No, but we are considering using such tools
- No - we are not considering the use of such tools





## The perceived value of ITRM

In today's business environment, organizations need to demonstrate value from the procedures they put in place - whether they have arisen from recent investments or not. In addition to the risk management value, we asked the participants in the IT Risk Agenda Survey to rate the effectiveness of their ITRM processes against that of their competitors. The results show that organizations with 'mature' ITRM rate the effectiveness of ITRM much more highly than peers. In our view these organizations use their ITRM program to obtain competitive advantage: we know that there is a strong correlation between the length of time an ITRM program has been in place, and its superior effectiveness against

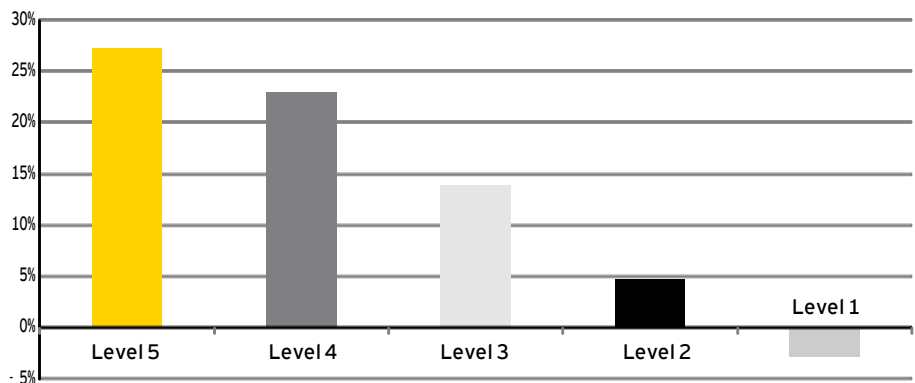
competitors. This can translate into reduced reputational risk, improved stakeholder confidence and more preferential ratings from outside commentators and regulators.

Added value can also be demonstrated in other ways: our results show that organizations that have more 'experience' in ITRM, through years of a more established program, are more risk alert and more attuned to the changing trends in IT risk. They may have higher standards and expectations for their program and so work harder to stay ahead of IT risk, rather than keep up with it.

Those that are not considering a program are more likely to be ambivalent as to whether IT risk is more challenging or not. This could suggest a greater degree of complacency or a greater lack of awareness versus those organizations that have a program.

### How would you compare the effectiveness of your organizations' ITRM with that of your competition? (% participants responding 'ours is more effective' )

- **Level 5**  
The program has been well-established for several years
- **Level 4**  
We introduced a program within the past three years
- **Level 3**  
We are in the process of implementing a program
- **Level 2**  
We are currently evaluating options for a program
- **Level 1**  
We are not considering a program



# Taking action

The evolving landscape clearly argues for an in-depth review of business and IT risks and corporate strategy around the key megatrends of consumerization, cloud computing, business continuity, cybercrime, internal threats and the accelerating change agenda. For example: a review of data management and remote working policies could be undertaken to see whether the IT function could manage any future risks arising from new mobile technologies and the use of social media today. This may drive an initiative to get on a more forward, pre-emptive footing. An organization should ask itself whether it is geared up to merely cope, limit the damage and allow business continuity or whether it is actually geared up to prevent an incident occurring in the first instance.

If the CIO or the overall board needs more evidence, a competitor evaluation would be a good place to further clarify the value to be gained from the implementation of ITRM. Alternatively, an incident at a key competitor could be used as a scenario to determine the impact on their own organization - with particular focus on the impacts on revenue and value, which may help to overcome budget considerations.

In any case, ITRM work needs to be far-reaching and thorough. The evolving nature of the IT risk landscape means that organizations must continuously monitor whether they have become significantly 'out of step' with the nature of today's threats, and in comparison to their industry peers are vulnerable to reputational and brand asset damage.

We therefore propose the following next steps that organizations could embrace to take ITRM into action:

## Taking action: next steps to improve and implement ITRM

After reading this article, could you answer the following questions for your organization?

### Enabling business performance

1. What are the typical risks in your industry impacting your business performance?
2. How important is ITRM as part of your overall risk management?
3. Do you understand how better ITRM can improve the performance of your business?

### Focus on the IT Risks that matter

4. Do you understand the mode that (parts of) your organization are in: 'factory', 'strategic', 'support', or 'turnaround'? What are the key risk areas?
5. How do the 6 mega trends in IT risk affect the IT risks your organization is facing?
6. Do you have an accurate perspective on the use of mobile devices and social media by your employees in conducting their work? Especially with regards to the flow of company data and potential data leakage?

### Your ITRM program

7. How prepared is your company management to embrace IT risk as a firmwide challenge? Are you focusing on your key risks and do you direct your spend to the risks that matter?
8. Are you continuously evaluating IT risks?
9. Does your ITRM program cover all the components discussed on pages 12 and 13 of this report?
10. Are you aware of the maturity of your ITRM program? What needs to be done to bring your program to the next level?
11. What role can enabling technologies play in your ITRM program?

## About our IT Risk Agenda survey:

Working with the Economist Intelligence Unit (EIU), we carried out a survey of attitudes to IT risk in major organizations across the world. During June/July 2010 online interviews were completed with 818 senior executives within the IT function (48% CIOs and 52% CTOs). The companies were from all major business sectors: manufacturing, utilities, media, retail, technology, healthcare, transport, agriculture, and professional and financial services. Each organization had global annual revenues in excess of US\$500m, and the annual revenue of more than half of the companies surveyed was between US\$1b-10b. Each organization employed between 100-1,000 full-time IT staff globally.



**About Ernst & Young**

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 141,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit [www.ey.com](http://www.ey.com)

**About Ernst & Young's Advisory Services**

The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk. Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference. Our 20,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and superior client experience. We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that to achieve your potential as an organization you require services that respond to your specific issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where the strategy is delivering the value your business needs. It's how Ernst & Young makes a difference.

© 2011 EYGM Limited.  
All Rights Reserved.

EYG no. AU0886



In line with Ernst & Young's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

[www.ey.com](http://www.ey.com)

## About Ernst & Young

**At Ernst & Young, our services focus on our individual clients' specific business needs and issues because we recognize that each is unique to that business.**

IT is a key to allowing modern organizations to compete. It offers the opportunity to become closer to customers and more focused and faster in responses, and can redefine both the effectiveness and efficiency of operations. But as opportunity grows, so does risk. Effective ITRM helps you to improve the competitive advantage of your IT operations, by making these operations more cost efficient and managing down the risks related to running your systems. Our 6,000 IT risk professionals draw on extensive personal experience to give you fresh perspectives and open, objective advice – wherever you are in the world. We work with you to develop an integrated, holistic approach to your IT risk or to deal with a specific risk and information security issue. We understand that to achieve your potential you need tailored services as much as consistent methodologies. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

For more information on how we can make a difference in your organization, contact your local Ernst & Young professional or a member of our team listed below.

### Contacts

**Global**

**Norman Lonergan** +44 20 7980 0596 [norman.lonergan@uk.ey.com](mailto:norman.lonergan@uk.ey.com)  
(Advisory Services Leader, London)

**Paul van Kessel** +31 88 40 71271 [paul.van.kessel@nl.ey.com](mailto:paul.van.kessel@nl.ey.com)  
(IT Risk and Assurance Services Leader, Amsterdam)

**Advisory Services**

**Robert Patton** +1 404 817 5579 [robert.patton@ey.com](mailto:robert.patton@ey.com)  
(Americas Leader, Atlanta)

**Andrew Embury** +44 20 7951 1802 [aembury@uk.ey.com](mailto:aembury@uk.ey.com)  
(Europe, Middle East, India and Africa Leader, London)

**Doug Simpson** +61 2 9248 4923 [doug.simpson@au.ey.com](mailto:doug.simpson@au.ey.com)  
(Asia-Pacific Leader, Sydney)

**Naoki Matsumura** +81 3 3503 1100 [matsumura-nk@shinnihon.or.jp](mailto:matsumura-nk@shinnihon.or.jp)  
(Japan Leader, Tokyo)

**IT Risk and Assurance Services**

**Bernie Wedge** +1 404 817 5120 [bernard.wedge@ey.com](mailto:bernard.wedge@ey.com)  
(Americas Leader, Atlanta)

**Paul van Kessel** +31 88 40 71271 [paul.van.kessel@nl.ey.com](mailto:paul.van.kessel@nl.ey.com)  
(Europe, Middle East, India and Africa Leader, Amsterdam)

**Troy Kelly** +85 2 2629 3238 [troy.kelly@hk.ey.com](mailto:troy.kelly@hk.ey.com)  
(Asia Pacific Leader, Hong Kong)

**Giovanni Stagno** +81 3 3506 2411 [stagno-gvnn@shinnihon.or.jp](mailto:stagno-gvnn@shinnihon.or.jp)  
(Japan Leader, Chiyoda-ku)