



cutting through complexity

# Technology Risk Radar

## 2nd Edition

[kpmg.com](https://kpmg.com)

---

### **What happened in the last year?**

Price tag for an IT incident

*Page 05*

### **Looking forward - Financial Services**

Top ten risks and why

*Page 11*

### **Responding to technology risks**

*Page 25*

---



# Introduction



Jon Dowie



Kiran Nagaraj

Technology failures, data losses and other incidents are increasingly in the news. How does one filter through the noise? In this second edition of the Technology Risk Radar, we seek to apply data analytics to better understand the evolving risk landscape.

We analyzed and evaluated more than 10,000 news articles related to IT incidents from around the world over a 12 month period starting from September 2013. We then surveyed KPMG industry specialists and asked them to provide a forward-looking perspective on the top risks which they believe their industry or sector will face in the next three years. We then conclude with some practical tips from our risk management specialists on what organizations can do to address some of these risks.

Why does this matter? Technology is no longer a functional area within a business operating in isolation. Those days are long over. Increasingly, businesses are seeing themselves first and foremost as technology companies, with the technology sitting at the center of the value chain and their core operations. The fact that technology is at the heart of everything we do, makes it all the more crucial for businesses to understand the risks associated with IT — first their cause, but just as importantly, how they can be managed, mitigated or avoided.

Based on feedback from our readers and our clients, we have extended both the scope and the methodology of our analysis from last year to present a broader picture that can help business leaders focus on the main threats to which technology can leave them vulnerable. Cyber security-related risks still dominate some industries. But, as the findings clearly suggest, other core technology risks — such as availability and quality — need to be brought to the fore.

Past incidents can provide an indication of the risks that organizations face regarding their technology systems and infrastructure. Together with a forward-looking perspective and risk mitigation options, we hope this report will be a useful tool in informing risk assessment activities and prioritizing risk mitigation investment, as well as benchmarking.

---

The Technology Risk Radar is relevant — indeed essential — reading for a wide audience. The most likely readers are Chief Information Officers, Chief Risk Officers, Heads of Audit and Chief Operations Officers. It's also vital reading for those with an interest in technology risk and control, including Executive and non-Executive Directors.

Our message to these readers, based on our findings and our experience, is that organizations need to do more to avoid the avoidable and exercise better control over their technology environments, processes and people. The only way to achieve this is by elevating the profile of technology risk. We have already seen some organizations use technology risk management not only for value protection, but also to drive competitive advantage. We believe that this will be the way forward.

Investments in technology will continue to rise as businesses embrace digital and other opportunities, but this needs to be matched by investments in assessing, managing, mitigating and monitoring the associated risks. At a time, when even our regulators have shown themselves to be vulnerable to technology risk, no one can afford to be complacent.

**“We hope this report  
will be a useful tool  
in informing risk  
assessment activities  
and prioritizing risk  
mitigation investment,  
as well as benchmarking.”**

# CONTENTS

## Media-reported events

What happened?	05
What were the causes?	07
Which industries were affected?	09

## Looking forward

Financial Services — Top ten risks	11
Suppliers and the extended enterprise	13
Governance and oversight for tomorrow's technology	15
Troubles with IT transformational change	17
Harnessing data for competitive advantage	19
IT spending on compliance at the expense of business priorities	21
Regulatory non-compliance	23

## Responding to technology risks

Building a risk management capability	27
Cyber security	29
Building resilience	31
IT for risk	33

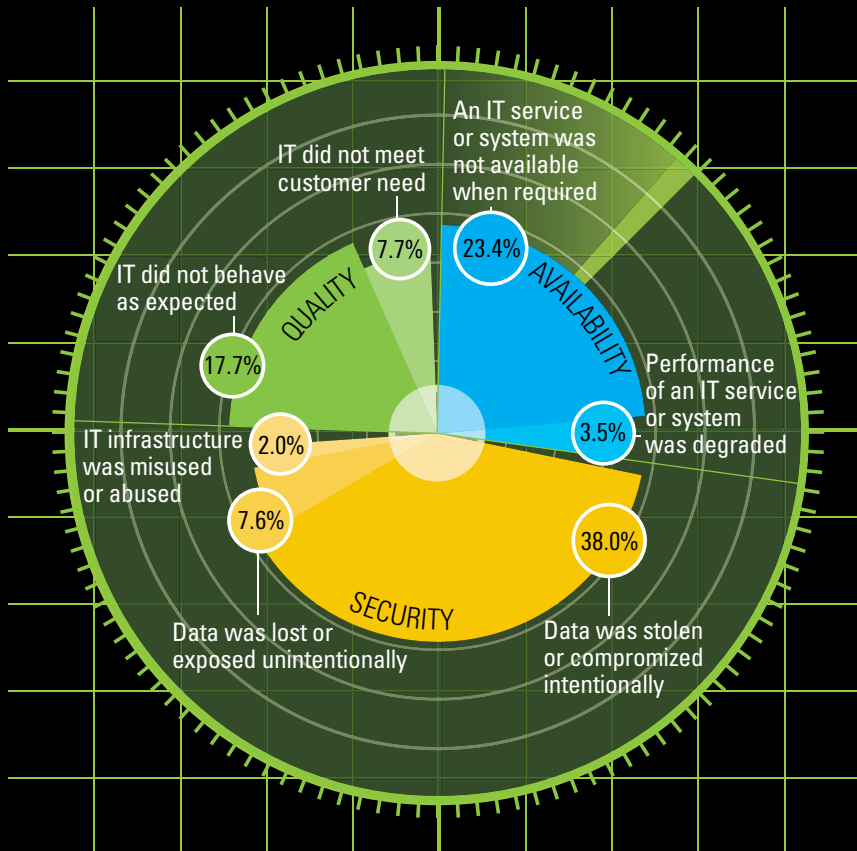
# Media-reported events





# MEDIA-REPORTED EVENTS: KEY FINDINGS

## What happened?



One of the most interesting findings is that while cyber security tends to be the attention-grabbing element of IT risk, security-related incidents accounted for less than half of the total number of incidents.

The very term “security” usually conjures up visions of theft. And yet a considerably large number (nearly 16%) of the security issues involved the unintentional loss or exposure of data. This proportion is even higher in some industries — almost 36% in Healthcare & Pharmaceuticals. These statistics are alarming as these incidents must arise from a failure of internal controls — checks which should be a basic element in any security control system, technological or otherwise. Cyber security continues to be a key area of concern for organizations. Later in this document, our cyber security specialists provide some practical insights on how organizations can protect themselves and better prioritize their investment in this area.

Availability accounted for about 27% of all incidents in our analysis. Financial Services and Technology were the two industries with the highest proportions (more than 34%) of incidents related to availability. You may be thinking: what about the incidents that didn’t make the news?

• Some incidents may have resulted in more than one type of impact (e.g., an incident could have caused data loss and service outage)

Indeed, internal operational failures aren't typically made public. It is clear from our analysis that the incidents that do make it into the news may just be the tip of the iceberg. While regulation in some industries requires that a loss of data or data theft be disclosed, there is generally no such requirement for internal operational failures such as server outage. So, given that the lack of availability is a top risk facing organizations, what approach should companies adopt to address this? Later in this document, our specialists discuss some ideas to improve technology resilience.

More than one-quarter of incidents concerned IT quality issues. We believe that this proportion will rise as businesses introduce new technology to digitize more of their processes. Risks change in step with the introduction of new technology platforms and processes — and so should the investment to manage and deal with the resultant risks. The right level of technology governance and program management capabilities should enable an organization to deliver its technology projects on time, to budget, and to requirements, creating a win-win situation for all the organization's stakeholders.


Many already recognize that IT risk is about much more than cyber security. Our findings help reinforce this view. The results from the Radar emphasize the need for organizations to take a more integrated approach to any technology risk management exercise and make sure they fully consider the risk landscape. Availability and quality considerations should not be over-looked. Indeed, we have seen a focus by some regulators on resilience and system availability.

Technology risk management is very much about protecting organizations from direct and indirect financial impact. From our analysis, we estimate that on average, an IT incident can cost the affected organizations over \$642,000 — slightly higher than the average cost of a data breach as estimated recently by the Ponemon Institute. While media-hype continues to focus on the generally more sensational and emotive incidents such as cyber attacks and data breaches, our analysis suggests that system outages and IT quality issues can prove to be just as costly for organizations.

#### By the numbers

 **\$642,000**  
Approximate price tag for an IT incident

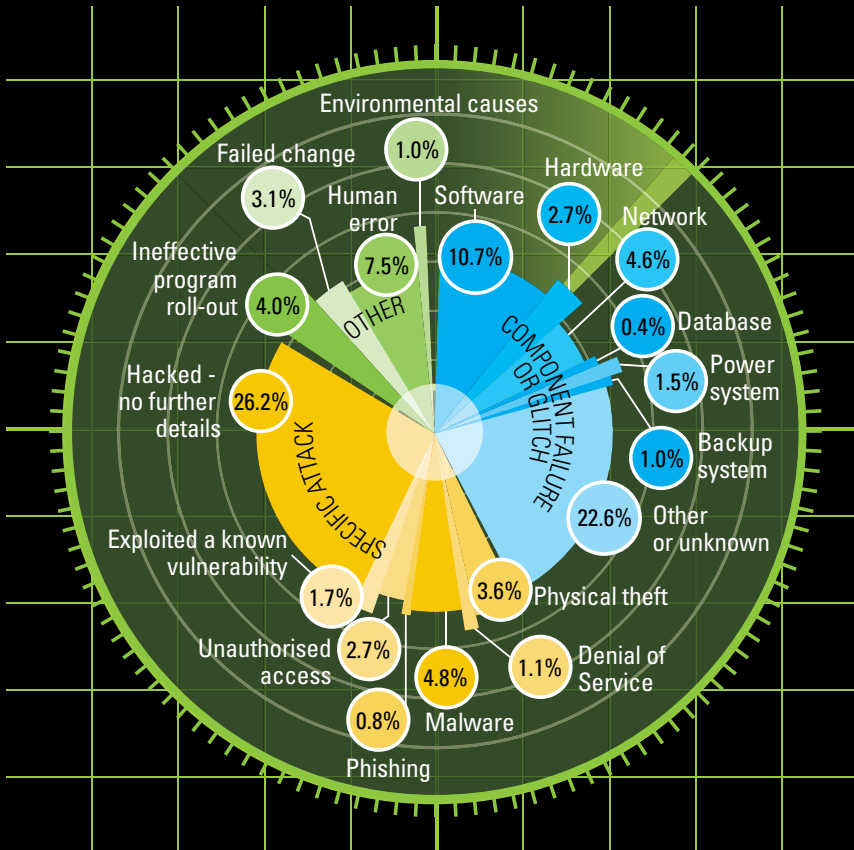
 **4 million**  
Average number of financial accounts (e.g., credit cards) affected by an IT incident

 **776,000**  
Average number of people (e.g., individuals, patients, employees) affected by an IT incident

• Based on a subset of incidents which had relevant data publicly available

# MEDIA-REPORTED EVENTS: KEY FINDINGS

## What were the causes?



We found that a shockingly high proportion of incidents were caused by factors generally considered as “avoidable”. Avoidable causes such as component failures, program or change failures and human errors led to more than one-half of the incidents. These are considered avoidable as component failures, for example, can be prevented by taking the right precautions, exercising vigor on testing components and building the right level of resilience to enable fail-over.

The leading culprit for component failures was software. Where information was available about the specific component that failed, nearly one-half (51%) related to software. Organizations could implement better testing practices and improved software quality management approaches (including for outsourced services) that can reduce this risk.

Specific attacks continue to be a major threat. But it’s worrying to see that a number of organizations still aren’t getting some security basics right. Physical theft was surprisingly high, accounting for about 24% of cases where the cause was a known type of specific attack. Physical security is generally thought to be a mature control area for organizations, but it would appear this is not always the case.



---

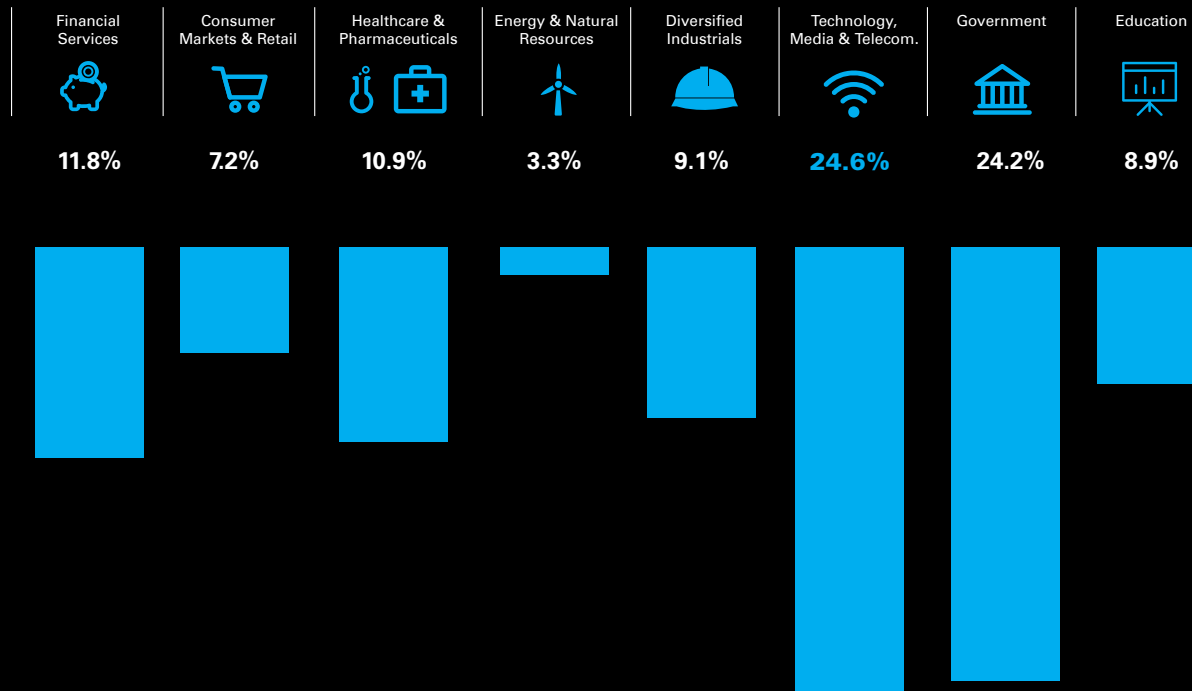
Human errors (e.g., information sent to wrong recipient, data entry error, etc.) contributed to more than 7% of incidents — a high proportion given that in today's digital age many controls are automated. Any investment in technology should be accompanied by investment in training and awareness — a point which a number of organizations have clearly ignored to their cost.

There's a common theme which runs through the incidents described here — the importance of better risk management and controls. There is little an organization can do to avoid being attacked by hackers. But all organizations can continually monitor their risk safeguards and prioritize action against IT risks. Later in this document we talk about the need for better governance and oversight, particularly for tomorrow's technology. We also discuss how to build a better risk management capability to ensure the business, its customers, the Board and IT itself are protected.

*Avoidable causes such as  
component failures,  
program or change failures  
and human errors led to  
more than one-half  
of the incidents.*

# MEDIA-REPORTED EVENTS: KEY FINDINGS

## Which industries were affected?



**The top three industries affected were the same as last year, although their rankings have changed.**

Technology has now the dubious privilege of being the industry most affected by IT incidents, according to our research. The growth of the Internet of Things and the ubiquity of devices suggest that this industry will keep this top spot for some time.

In second place is Government, with this high ranking probably because technology failures at government bodies often impinge on the general public, meaning that the media gets to hear about them.

Financial Services has moved down to third place. While we believe that the industry is getting better at managing IT risk, the impact of individual incidents may be on the rise. We observed that, on average, about 4 million FS accounts (e.g., credit cards) are affected by an IT incident.

This point relates also to other sectors. For example, one very high-profile incident in the Retail sector generated hundreds of news articles, and affected around 40 million people. And yet in our study this counts as one incident. So while the total number of incidents in Retail is lower than for Government or Financial Services, the impact might well have been proportionately higher.

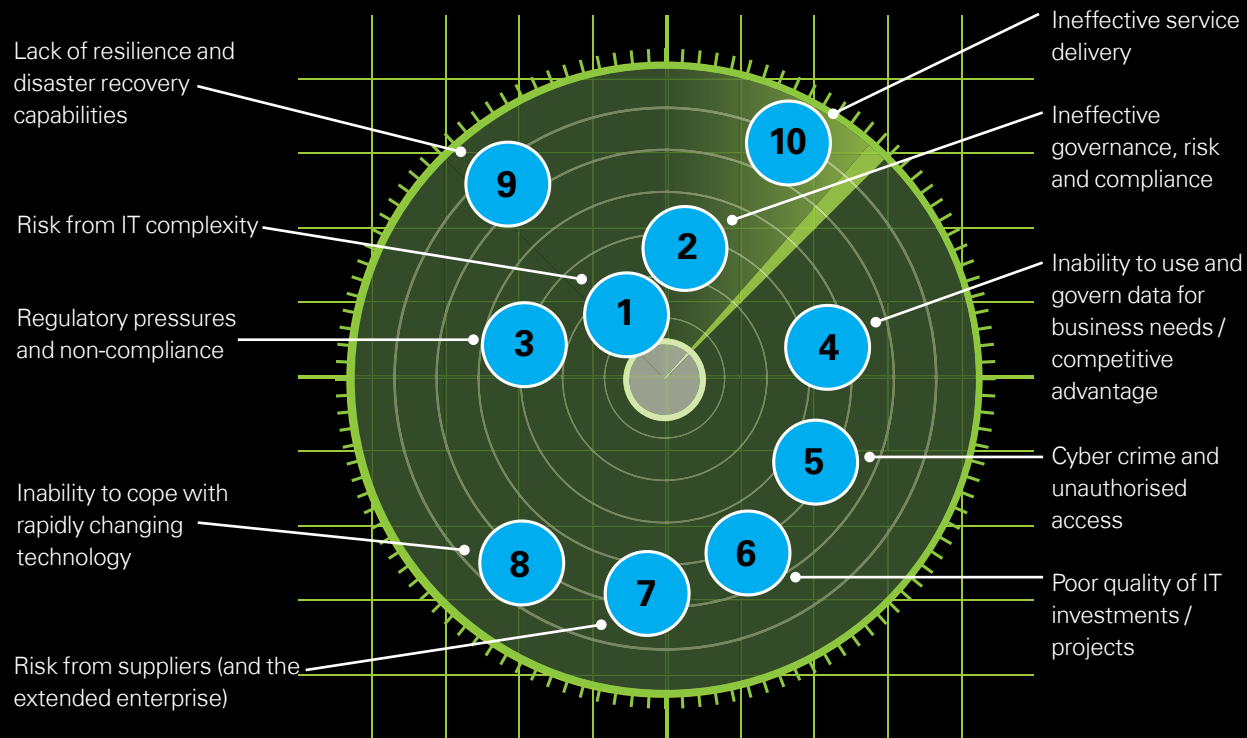
What is also interesting is that specific types of incidents are affecting some industries more than others. For example, Financial Services and Technology had a higher proportion of availability-related incidents than any other industry.

---

# Looking forward - Financial Services



# LOOKING FORWARD - FINANCIAL SERVICES: TOP TEN RISKS



**Past incidents can provide an indication of the risks that organizations face over their technology infrastructure. But, where should Financial Services organizations prioritize their future investment in risk management?**

We surveyed technology risk specialists across KPMG member firms' Financial Services practice globally to obtain an insight into what they believe the biggest technology risks facing the industry will be over the coming years. The top ten most popular responses can be found to the left.

Much of the top ten remains unchanged from last year. However, the inability to cope with rapidly changing technology and failure to use data for competitive advantage now figure as top risks for Financial Services organizations.

---

*We asked a number of industry specialists from KPMG's global network of member firms to tell us which of the top ten, in some shape or form, will be the biggest technology risk facing the Banking, Insurance and Investment Management sectors and why. Over the following pages, they provide their answers.*

---

# Looking forward - Banking

Q. What will be the top technology risk facing the Banking sector in the next few years?

A. Suppliers and the extended enterprise



David DiCristofaro  
*KPMG in the US*

**As the business environment grows increasingly complex, banks will rely more and more on third parties to carry on their business and serve their customers. For this reason, I believe that third-party security and data privacy will be among the top risks facing the banking sector within the next three years.**

Banks everywhere are under pressure. It is hard for them to grow organically in the post-crisis period, while increased regulation imposes costs and limits capital available for external growth. With turnover stagnant, banks have to concentrate on driving out costs and finding new ways to drive growth.

This is where service providers and other intermediaries play an important role — and where external risk factors come in. And it is why any bank relying on third parties needs to make sure that the controls and compliance bar is set as high at its service providers as it is within the bank's own systems and procedures.

This is not an option — regulators are increasingly expecting ever more oversight of third parties. Rationalizing relationships by cutting numbers and consolidating external suppliers can help (although there is a fine balance between having a manageable number of suppliers while not being dependent on too small a number). Banks should also focus on the underlying contracts related to their supplier relationships, and on monitoring their suppliers' organizational control reports or exercising other kinds of validation procedures over their controls and compliance.

The resulting exposure from lapses in data security and privacy at third-party providers poses a serious threat to individual banks. This risk extends down throughout the banking supply chain, where a security or privacy incident at a bank as a result of a third-party error in one of their suppliers can signal the end of the service provider. And in a worst case scenario, if a major provider whose services were used throughout the industry were to have a problem, then the domino effect would cascade throughout the world.

I believe that these risks will also impact smaller banking institutions, possibly disproportionately. These institutions may rely more on third parties for their core banking capabilities than a larger bank does, plus they might not have the resources to be as proactive over validation of third-party controls and compliance.

What will banks do in response to these risks? I believe that the industry is forward-looking enough to draw risk out of the service provider community. The major service providers are certainly motivated to step up to the challenge. As their business becomes more complicated, it will be in their best interests to be on the cutting edge of how they mitigate the risk for fear of being shut out of the market. They will find ways to innovate, such as through security analytics, to seek out and prevent risk events occurring.



I think that the right roles already exist within most large banks to mitigate this risk. The challenge will be around governance and communication between the people on the business, technology and compliance sides, and the constantly changing nature of the banking supply chain. The focus will be to own supplier relationships and risks across the supplier life-cycle and across the enterprise — quite a challenge given that often several different functions have a relationship with one supplier over each one of the many aspects of the business. Banks are looking at ways to improve this, and certainly the regulators are expecting it. Many of our clients are on this journey, and I believe that this will be an enduring trend in the management of their technology risk.

**The challenge will be around governance and communication between the people on the business, technology and compliance sides, and the constantly changing nature of the banking supply chain.**



# Looking forward - Banking

Q. What will be the top technology risk facing the Banking sector in the next few years?

A. Governance and oversight for tomorrow's technology



Michael Elysee  
KPMG in the UK

**I believe that banking products will be fundamentally transformed over the next three years, driven by changes in technology. Banking is now becoming a digital industry — as evidenced by recent announcements about changes in the number of high street banking branches — and the banking industry and customers need to accept this fact.**

The question is whether the banking industry can develop skills fast enough to keep up with the speed of technological change, and properly manage the many associated risks. I believe that the level of technical experience required, particularly within risk functions, will be on a scale we have not seen before. And I fear banks will have trouble keeping up with the pace of change — never mind pre-empting it.

Quite simply, those charged with governance of banks are generally not yet equipped with the skills and experience to provide the right oversight, to properly question tech-driven banking products and to assess the risk management over these products. A few banks do have board members who can ask the right questions, while others ask consultants to provide that challenge. But I believe that the vast majority of them are simply not currently set up to manage the risk around their products.

I believe that every financial services organization needs a non-executive director who understands deep technology risk and is able to challenge business strategy. I wonder whether many audit committees actually have the right level of expertise to challenge technology risk matters, in the same way that a decade ago they didn't always have the right level of expertise to challenge product development.

Part of the problem is that over the past seven years or so the industry-wide pressure has been on regulation and control rather than investment in technology. Fallout from the financial crisis means banks aren't growing their top line but are focusing on the bottom line by cutting costs. There has been a drastic underinvestment in technology overall in the last decade. Legacy systems are rife, based on old technology, which cannot provide the kinds of functionality and security required of modern systems.

We are starting to see banks acknowledge that they need to increase their levels of investment and expertise. Security breaches and data loss help to focus attention - banks don't want to be the organization on the front page of the newspapers for the wrong reasons. When they read about others making headlines for these reasons it's not with a sense of Schadenfreude, but rather "there but for the grace of God..."

But while there is a sense of needing to get up to speed, I believe more action must be taken and fast. Hackers are moving quicker, cracking security measures more rapidly, and forcing banks to play catch up. Banks need to address risks during the development phase of their new technologies if the industry is going to shift from being reactive to proactive with its tech risk.

---

Some 20 years ago banking products were supported by technology and what followed was a period in which the products were enabled by technology. Now we're in a situation where technology is overtaking the business and will determine what the business can do — and where it is headed.

I believe that competitiveness between banks will determine how they take advantage of technology over the next three to five years. Banks have to invest; I don't think they have any choice. The disruption will be huge — on par with that which caused the regulatory changes we are seeing post the financial crisis. But banks have no option — they must adapt or die. What they do around the management of the risks that arise from this scale of change will be key to their success.

**I believe that the level of technical experience required particularly within risk functions will be on a scale we have not seen before.**



# Looking forward - Insurance

Q. What will be the top technology risk facing the Insurance sector in the next few years?

A. Troubles with IT transformational change



Jon Dowie  
*KPMG in the UK*

**I believe that the insurance industry will face an immense challenge in implementing its strategic IT transformational change agenda over the next three to five years. While I think that the insurance industry stands ready and willing to tackle the challenge, the fundamental question is — do boards recognize the issues, the constraints and the challenges that executing the strategy will bring? Quite simply, I don't think they do.**

But I believe that there is a real threat that resources and management focus will once again be distracted and diverted by the final stages of the implementation of Solvency II in time for January 2016. All insurers will struggle with ever more urgent requests for money and expertise as insurers balance the competing demands of the IT and compliance change required. The same subject matter experts will be called upon to execute IT transformational strategies and deal with Solvency II simultaneously, leading to a perfect storm of calls on these experts' time to deliver both vital imperatives.

I'm also not convinced the industry is ready for the IT revolution it needs yet. I believe that certain digital transformational fundamentals — in particular data governance and management — are not in place. Many insurers have simply not invested in this, leaving their businesses with disparate, incomplete and poor quality data sets. If companies have not got their arms around their customer data, or if it's not appropriately organized, managed and governed, then they will quickly find that their strategy unravels.

And let's not forget the rapid and accelerating pace of change across the business landscape as a whole. Implementing complex, multi-year projects that take an age to deliver simply won't work anymore — by the time these are complete the market will have moved on.

Instead, insurers need to start by recognizing that previous ways of working are too slow and cumbersome in the current world. They need to be able to introduce systems and infrastructure which are agile and which they can adapt quickly to bring new products to market, and to move into new markets. Some companies are creating new organizations within their group structure to achieve this, so that rather than being constrained by historical legacy they are effectively creating their own start ups; this is a positive development.

I believe that insurers will see that the future lies not in developing customized solutions in-house, as they have done in the past, but that they will use the expertise of software development houses and external partners to implement their technology transformation in a more rapid and effective manner. There is much more choice available for insurers than ever before, with several out-of-the-box software solutions having come onto the market recently.

There is also much more agility in place through the use of cloud based infrastructure, applications and services. These enable insurers to purchase externally and configure to their needs while being flexible to meet future changes — precisely what these institutions need.

The risk, I fear, is that insurers will not be able to see these projects through to a satisfactory conclusion. If they do nothing, they will be left behind — that's for sure. But if they execute change badly, or are unable to execute properly because of resource limitations, they will also fail. Insurers must recognize the restrictions on skills and capabilities within their own organization, and build flexibility into their systems design. And they must move fast so they are not at the tail end of change, stuck with the resource remnants that turn their transformational dreams into nightmares.

**While I think that the insurance industry stands ready and willing to tackle the challenge, the fundamental question is — do boards recognize the issues, the constraints and the challenges that executing the strategy will bring?**



# Looking forward - Insurance

Q. What will be the top technology risk facing the Insurance sector in the next few years?

A. Harnessing data for competitive advantage



Phil Lageschulte  
*KPMG in the US*

**I believe that the single biggest technology-related risk facing the insurance sector is related to data - and more specifically to the insurer's ability to use data competitively; and to effectively and responsibly manage the integrity, protection and governance of that data.**

Insurance companies are in the risk management business, and their assessment of risk relies almost exclusively on information. Within their highly competitive environment, the more reliable information insurers have, the better able they are to evaluate, select, reject, segment, and underwrite their risk decisions efficiently.

The volume, velocity and variety of data available to insurers continues to grow at a staggering rate. This much is clear. But I believe the danger lies in companies not collecting the best, most relevant information available and, if they do, not capturing the full value from it. The question they need to ask is whether they can distill value from the noise — and how much data is too much?

Many insurance companies have historically suffered from disaggregated systems (and therefore data), with little or no link between the systems over each of their business lines, financial reporting, underwriting and claims management. This situation has improved, but experience suggests we still have a long way to go.

Within these diverse systems, the key to data management is what I think of as the single version of the truth — the data warehouse on which a common infrastructure resides. This hosts the company's internal data on its customers, and the external data which it buys from data management companies.

But there is a third component to data — unstructured data based on publicly available information on customers. For example, a fire insurer will have internal data on the address insured and can purchase some external data on the policyholder. But additional data could include the location and access to the nearest fire station. The insurer can determine whether the property is two miles from a fire station, or 20. Understanding how quickly a fire service can respond to and limit property damage can make a big difference to the risk equation, and hence to risk selection, cost reduction, and premium pricing.

I believe that aggregating, collating and using this data will give insurance companies an immense competitive advantage over the next few years by enabling them to provide services tailored more effectively to customers' circumstances and risks. But to gain this advantage they need to be far more visionary in their approach to collating and using this data. Other types of business are building risk command centers to monitor external chatter. I believe insurers must do something like this to help identify activity, history or other data around individuals.

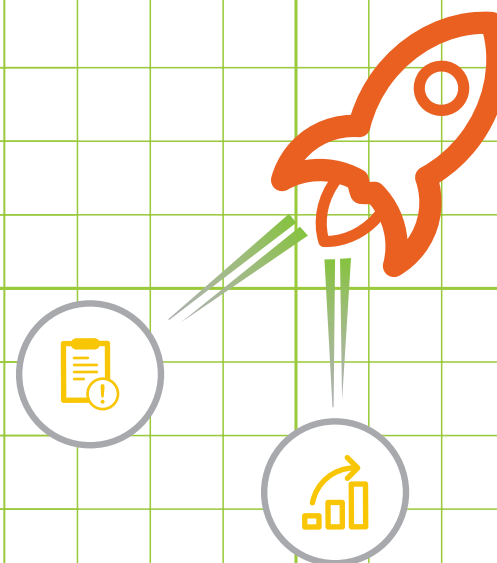


At the same time, regulators are keeping a careful watch over consumer privacy. I believe that as they try to balance protecting consumer privacy without stymieing consumer value, they will consider whether insurance companies can effectively self regulate by showing that they can protect internal and external customer information and use it appropriately without putting customers at risk. If insurers can do this, regulation growth will be curbed.

Meanwhile, I believe that a new role will emerge in insurance firms — that of the Chief Data Officer. This is a role we are starting to see appear in other industries, and it is inevitable we shall see this in such a data-rich industry as insurance. What will mark insurance from other sectors, I believe, will be that the current head of risk may take ownership of this role. Data governance tops many boards' agendas and is inherently associated with the risks that insurers manage, which is why it will be a natural evolution for the risk function to segue into data.

Data is the insurer's lifeblood. The amount and nature of data is growing exponentially. This is why I believe that the single biggest technology risk insurers face is around that data: the ability to accumulate and capture value from data which is out there but not currently available to them, and to protect and use that data responsibly. Unstructured data is starting to change the face of insurance, and companies need to step up to the line on this — or face extinction.

**I believe that aggregating, collating and using this data will give insurance companies an immense competitive advantage over the next few years.**



# Looking forward - Investment Management

Q. What will be the top technology risk facing the Investment Management sector in the next few years?

A. IT spending on compliance at the expense of business priorities



John Machin  
KPMG in the UK

**One of the biggest technology risk factors facing investment managers is the way in which IT spending is currently dominated by compliance-related activity at the expense of what may appear to be discretionary, but which is in fact necessary IT spending for other business priorities. I believe that even before the CIO can start to engage in a meaningful conversation with the business their book of work for IT is pretty much already written.**

Increasing regulatory and reporting requirements such as Dodd-Frank and FATCA in the US and the Alternative Investment Fund Managers Directive in the EU are placing greater demands on the ability of already struggling systems and processes to generate ever more accurate and timely information. The huge investment required to meet these non-negotiable requirements is leeching funds which might otherwise finance strategic priorities to reduce risk.

The most prominent example is the IT simplification agenda. Too many investment management organizations are already lagging behind here with a legacy of silo technologies supporting individual products, often created by acquiring others with slightly differing flavors of technologies, which have never truly been tackled. The resultant overblown IT landscapes are high on maintenance and inherent operational risk and desperately need rationalization.

Interjecting a third party into this already crowded environment, say for custodianship purposes, adds further complexity, challenging effective management and oversight. Distance between such third parties and the investment manager — in terms of level of oversight, language, commercial and cultural differences, often coupled with physical distance — can lead to problems with data quality, data loss, availability and confidentiality.

The intricacy and diversity of tailored products, coupled with the sheer volumes of transactions, places high demands over data integrity on investment managers. Standardization and simplification of architectures would appear to be the only rational way to square this circle.

Seeking alpha in a time of meager market returns increases pressure on costs while reducing in-house talent levels, ironically when demand for knowledge and services may be at its peak. Market players may be forced to pool their meager discretionary resources in order to create a more viable total solution for the marketplace through the creation of utilities. My fear is that this strategy risks invoking the law of unintended consequences as parts of the operational jig-saw are placed increasingly outside the reach of the regulators in unregulated entities. And so the vicious circle continues.

Various regulators are starting to be worried about such unintended consequences but I cannot see anything changing their stance in the short- to medium-term — the over-riding geopolitical and economic fears are simply too strong to ignore.

However, with regulatory-driven activities (such as legal entity rationalization or recovery resolution planning) now swallowing as much as three-quarters of typical IT spending, under-investment in rationalizing the architectural landscape will probably be fact of life for some time to come.

And at a time of ever increasing threats, such as cyber security, boards and executive management struggle to make truly informed risk-based decisions determining their true business priorities and sticking to them.

This is why I believe that investment management firms face their own internal investment management crisis in terms of their technology expenditure. Such constraints mean they might not pay due attention to the business risk lessons from the sins of their past, which could ironically be a waste of a good crisis. Boards must understand that IT can, and should, play a serious role in mitigating these risks — providing there is funding for comprehensive and integrated business-driven solutions, and not those created purely to satisfy regulatory requirements.

**The huge investment required to meet these non-negotiable requirements is leeching funds which might otherwise finance strategic priorities to reduce risk.**



# Looking forward - Financial Services

Q. What will be the top technology risk facing the Financial Services industry in the next few years?

A. Regulatory non-compliance



Daniel Gorton  
*KPMG in the UK*

**I believe that regulation is, and will continue to be, the biggest technology risk factor facing financial service companies. As the number of regulations has rocketed, so financial services companies have built technology solutions to meet the systems and data challenges embedded in each new compliance. As a result, technology risk is now at the heart of compliance risk — both from the perspective of daily operations and as the engine for compliance. If your IT doesn't comply with regulation and if your IT doesn't enable compliance - then you won't comply.**

Much of the problem stems from the sheer volume and diversity of changes to regulation, and how organizations have managed this change. Typically, organizations have created a new project, program and solution to address each individual compliance need, and then run that solution in splendid isolation. Eventually this house of cards has to collapse — it is simply too difficult to manage all of these things separately.

I believe organizations need to take a holistic approach to compliance management which properly considers the interplay and overlap — and, just as importantly, the differences — in regulatory requirements. Only then can companies approach their new compliance efforts in a joined up way rather than building inefficiency upon inefficiency with every new layer of systems designed in isolation to meet the growing compliance burden.

The current state of compliance operations is the opposite of this strategic approach. Companies are simply so busy managing their existing regulatory cycles that they don't have the capacity to step back and take the holistic view needed. I believe that the only sensible answer is to be prepared to spend, to devote enough time, resources, capacity and capability to a team separate from day-to-day compliance management and from new regulatory projects, so that they can step back and start building a holistic compliance approach.

This way organizations can successfully continue to comply and have a realistic hope of operational efficiency, and maintain that efficiency as regulation becomes more and more onerous.

We have seen that compliance risk, as it relates to technology, is actually an umbrella term for all kinds of risk areas — project risk, information security, third party vendor risk and change management are just some of the areas specifically covered by recent regulation.

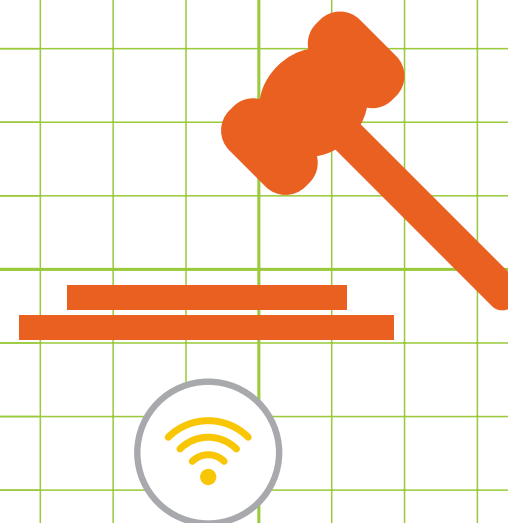
This is why I believe that compliance is the key technology risk facing financial services institutions. A material failure in any one of these areas may be enough to breach regulation, which inevitably leads to fines, remediation costs and intense supervision from the regulator going forward. I believe that organizations must deal with compliance strategically because it will save money over the long term.

My prescription of taking a strategic, technology-based approach to compliance has some upsides. If an organization does this successfully, then it can better assess and avoid, not only the impact and cost, but also some of the unintended consequences of proposed regulations. If organizations can more quickly and accurately understand the impact of proposed regulation on their business, they are in a much stronger position to influence the regulator on the specific requirements during consultation periods before implementation.

This should result in a more useful and mutually beneficial set of policies coming out of the regulator. Further, standardized regulatory data sets and formalized regulatory systems will enable organizations to influence other parties in the data chain by clearly articulating what can be provided, influencing the discussion from the start and hopefully suffering less change and upheaval as a result.

The costs associated with implementing a technological and integrated approach to compliance may seem high, but the risks are higher. Which company can afford to bear the escalating cost of compliance or the risk of failing to meet the regulators' requirements by misstating information, breaching compliance deadlines or failing regulatory reviews not to mention the adverse publicity that follows such regulatory failure? Good reasons indeed to use technology to enable compliance rather than be a risk to it.

**The costs associated with implementing a technological and integrated approach to compliance may seem high, but the risks are higher.**





---

# Responding to technology risks



---

*We also asked technology risk specialists from KPMG's global network of member firms to tell us what organizations should be doing to address some of these top risks. Over the following pages, they provide their answers.*

---

# Responding to technology risks

## Building a risk management capability



Jon Dowie  
*KPMG in the UK*



Kiran Nagaraj  
*KPMG in the UK*



Phil Lageschulte  
*KPMG in the US*



Vivek Mehta  
*KPMG in the US*

**With growing pressure from business partners, customers and regulators, IT risk management has emerged as a strategic business imperative for IT and risk leaders. Despite this, many IT risk functions continue to be under-staffed and rely too often on backward-looking processes and tick-box exercises.**

How can organizations move from this less-than-optimal situation to build a technology risk capability that is fit for purpose in the evolving risk landscape?

The first step is to strategize — to understand the starting point and the desired level of maturity. Many organizations who do IT risk well have been on this journey for many years. They follow a risk maturity curve, so over time their risk management flows from fire-fighting and reactive capabilities to being proactive, identifying risks before they hit, and using risk management to add value.

Business context is vital — without it, there will be little business value. After listing the technology risks that affect an IT entity (e.g., service, application, process, supplier), focus on the impact of each risk on the business. Then apply risk management practices.

Ensure the buy-in of all parts of the organization. Build a common risk language for use across all areas. Clearly define the set of services that the IT risk function provides and establish unambiguous lines of interaction with that function. Each department should view IT risk as a partner function and so the relationship should be treated the same way as that with any other partner.

All technology issues are underpinned by people, and risk management is no different. Staff the organization with the right people with the right skills, according to both your business and your technology needs. Keep investing in them to maintain staff as a key strength.

Execute your risk processes across the whole risk life-cycle — identify, manage, monitor, and mitigate. Some areas, such as cyber security and resilience, require more discipline so develop capabilities to perform deep-dives in these areas.

Over the years we have seen certain leading practices emerge in organizations that have created an effective function to respond to technology risks. One of the most fundamental of these is risk identification and measurement. Many organizations which do this well have built the infrastructure to aggregate risk information from different internal and external sources. They apply a combination of proactive and reactive techniques using top-down and bottom-up approaches to identify and measure risks. At the same time, they do not get lost in risk quantification, understanding that this cannot be done precisely — instead they focus on aggregating risk information and bringing the information to the right people.

They also integrate risk management fully into their existing IT governance bodies. Most organizations have IT governance bodies which serve as the decision making bodies for IT. IT risk should have a seat at this table. IT risk lives in the middle of IT and risk and so should have reporting lines to both. They utilize capabilities on either side whether it is extending current risk processes to IT, for example, or employing existing IT metrics to understand risk.

The core components of IT risk management are not new, but their effectiveness requires “risk” to be fully integrated with every IT attribute — strategy, architecture, development, operations, suppliers and data among others — seen in today’s organizations. Holistic thinking about risk management needs to start from the top and be fully in tune with the organization’s technology requirements. The role and the scope of the IT risk function should ultimately be driven by business objectives so it can function as the Chief Information Officer’s (CIO) “critical friend”.

**At the same time, they do not get lost in risk quantification, understanding that this cannot be done precisely — instead they focus on aggregating risk information and bringing the information to the right people.**



# Responding to technology risks

## Cyber security



Stephen Bonner  
*KPMG in the UK*



Ronald Plesco  
*KPMG in the US*

**Cyber security — it's the headline-grabbing and nightmare-inducing fear of every organization. But we believe organizations need to avoid the hype that surrounds breathless media reports of high-profile hacking or data theft events, and focus on the real threats and effective methods of militating against them.**

There is no denying that cyber crime is on the rise as our economies and lives become more digital. The threat landscape varies depending on the business or activity involved but can be a mix of fraud, espionage, political activism, or even individuals with a grudge.

So how can companies protect themselves? The bad news is that there is no foolproof protection against cyber attack. But organizations can make it a lot harder for attackers and block many of the less determined and sophisticated criminals.

Often this comes down to getting the cyber essentials right — a commitment from the top, action to raise awareness of the issue and basic protection measures around your core networks.

Then organizations need to go one stage further — be clear about what the heart of your business is and what needs additional protection. This might be intellectual property, financial or personal information, or continuity of operations. An analogy for what happens next is physical security in a hotel. Intruders may get into the lobby but you don't want them to get into the safe. So organizations need to put their most important valuables in the virtual back-room and ratchet up security accordingly.

An important dimension to cyber attacks that often gets ignored is people. Too often cyber crime is seen as a purely technical issue with a language all of its own. The reality is that many attacks come down to individuals — sometimes well meaning — who become the weakest link in the organization's defenses. Every business, every public sector body, every third sector association, should educate employees about security risks, how to spot possible viruses or hacking attacks, or unusual behavior among colleagues that point to a cyber attack from within.

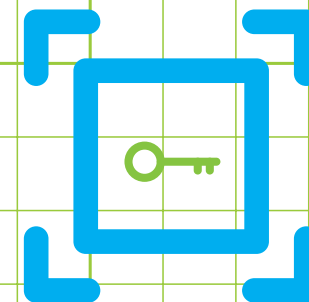
While protection is a vital first step, it isn't enough. But if safeguards fail, all is not lost. The smart response is to limit the damage an attack can cause as it happens. Having a fast incident response process and competent incident response team helps, but so does deft handling of media interest, addressing regulatory concerns and working to restore customer confidence, all as quickly as possible. Time after time, it isn't the incident itself which damages brand and reputation long term — it's the way firms handle themselves when it happens. So organizations need to think through what could happen before it does happen, be ready to exercise and test how to really respond in the heat of the moment, and make sure that decision makers understand their role in a crisis.

Importantly, this will help avoid knee-jerk reactions such as unplugging computer systems too quickly before it is clear what data has been stolen or damaged. That evidence may be needed in any subsequent investigation or even as a defense against future lawsuits from disgruntled customers whose personal information was stolen.

Most large companies have a budget for IT security, which is about between six and fourteen per cent of the total IT budget. That budget has grown over recent years but perhaps simple percentages mask the need to think about your exposure to cyber attack and strike the right balance between digital opportunity and cyber risk.

Cyber security needs to be core to every organization's discussions on new digital opportunities. Done right, cyber security can be an enabler, not a blocker, giving every business confidence to exploit opportunities by understanding risks and how to respond if the worst happens.

**Often this comes down to getting the cyber essentials right — a commitment from the top, action to raise awareness of the issue, and basic protection measures around your core networks.**



# Responding to technology risks

## Building resilience



Greg Bell  
*KPMG in the US*



Martin Lunt  
*KPMG in the UK*



John White  
*KPMG in the UK*

**Technology resilience is not just about technology. Its purpose is to enable a business to keep running, delivering its core products, services and activities, in the event of a technology-related disruption.**

Technology supports the resilience requirements of the business by being robust. But no longer does the technology department decide what needs to be done to keep business activities going — business now drives technology resilience, challenging how technology supports an organization's business needs.

The upshot is that organizations should stop considering technology resilience in isolation. Resilient technology is a necessary condition, of course, but it cannot provide a truly resilient business solution unless all other supporting factors around it are in place. Robust IT systems are pointless without foundations such as proper governance, processes, communications and training.

Where should an organization start in assessing its technology resilience? By taking a fresh look at how the technology it uses supports the business activities it delivers. By identifying business risks, both current and emerging, and evaluating the impacts of business process disruptions, an organization can prioritize its recovery requirements for critical business functions, including critical IT assets supporting those functions. Bear in mind that data recovery is just as important as systems recovery, and that IT can enable both processes.

A Business Impact Analysis (BIA) can help an organization identify critical processes and their dependencies across the business. This is typically done on an operational level, but we strongly advise it should also take place on a strategic level to protect organizational matters such as reputation, market share and market value. This calls for a co-ordinated response — different teams within the organization doing what they do best while working to a common organizational objective. Analysis of both the financial and non-financial impacts of business disruptions should drive the overall recovery requirements, including IT. The IT function should hold this data and help validate current recovery capabilities, identifying gaps against the business requirements determined through the BIA.

An effective disaster recovery plan must also understand third-party business partners and service providers' role in supporting the business functions, including those providing critical IT services. These third parties need to be fully evaluated when assessing IT recovery strategies to ensure there are no gaps or missing dependencies in the recovery strategy.

There has been a shift away from backing up data to physical tape due to developments in recovery technologies such as data replication, mirroring, virtualization of storage, servers and applications, through which the ability to rapidly re-deploy critical services in alternate locations has become the new standard.



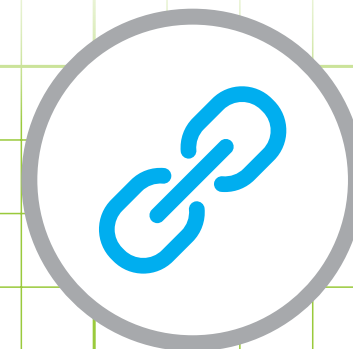
Leveraging these technologies enables companies to become more flexible and better equipped to respond faster in the face of an incident affecting critical technological infrastructure which vital business functions depend upon.

Cloud-based recovery services are on many organizations' radar as they offer a way to achieve advanced data recovery services at a more affordable, subscription-based price. There are concerns over security of the cloud but over time it will be a key component of every disaster recovery program.

These and other developments in technology have brought about a significant change in how organizations think about protecting themselves in the face of business interruption with a move from recovery to resilience ensuring a robust organization that can withstand and continue business with confidence.

The biggest challenge to achieving technology resilience is still cash. Technology costs serious money. Those in charge of the technology resilience need to be able to articulate clearly why their project is important and why spending resources will be effective, putting the idea of technology resilience into a business rather than a technology context. A BIA offers the means to build such a business case, as it represents a cost / benefit analysis to make data driven decisions around acceptable risk and technology recovery investment. Building a good business case for technology resilience can save money — and perhaps even save the business.

**Those in charge of technology resilience need to be able to articulate clearly why their project is important and why spending resources will be effective, putting the idea of technology resilience into a business rather than a technology context.**



# Responding to technology risks

## IT for risk



Daniel Gorton  
KPMG in the UK



Tony Torchia  
KPMG in the US

**Risk management should act as a critical friend to the business: understanding the organization's risks, assessing exposure against its risk appetite, then managing the risks in co-operation with the business. However, in reality risk management is usually either too close to or too far from the first line of defense, meaning risks which should have been mitigated against and avoided are all too often realized.**

Technology can be the perfect medium through which risk management can stay close to the business and bring together the three lines of defense, while simultaneously enabling compliance and business management. Today, we are starting to see risk tooling achieve some of these objectives. Risk management is evolving into a more integrated and repeatable process, rather than a series of staccato procedures. We are seeing an increase in the functionality of Governance, Risk and Compliance (GRC) systems, making them more useful across all three lines of defense, providing greater reporting and insight but also enabling continuous monitoring.

However, these early signs of truly co-ordinated risk management must be built upon if organizations are to reap the full benefits they are currently missing out on. Technology which enables continuous monitoring, analytics and real time reporting will help organizations to manage risks before they become issues. This can help save reputational damage, remediation activity and regulatory fines, issues which combined can cost businesses a staggering amount, especially in the context of a technology budget. Increased monitoring also means the business carries fewer risks, reducing risk capital and releasing money into the business.

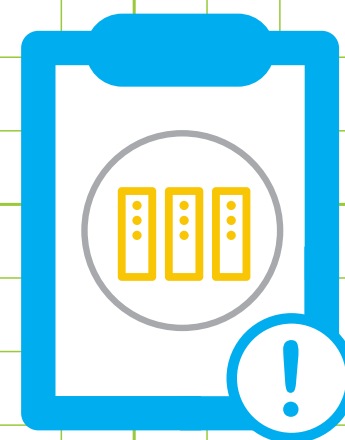
In addition, a business can use analytics powered by technology to assess if and where processes, controls and procedures are at odds with each other. This is particularly relevant to international organizations, which often see hundreds of local variations to what should be global processes and controls. Standardization can help reduce risk while saving money. Integrating risks and controls establishes a single version of the truth — vital when dealing with new regulations across jurisdictions and when getting to grips with the changing tenor of the global risk environment.

Pushing risk management into the first line of defense is the only way to enable prediction technologies to work effectively. Through building risk considerations into front-line systems, combined with automation and continuous monitoring, the business has a better chance of applying controls effectively, identifying potential problem trends and gathering data for analytics to learn more about its affairs. This goes to the heart of the value equation managing risk better and cheaper using technology — getting the right information into the hands of the decision makers by creating the right dash-boarding and visuals for the compliance, risk and control owners as well as the process owners.

Further, technology can also streamline regulatory compliance efforts. KPMG International's global risk survey showed today's businesses think their greatest risk is regulatory pressure — the onslaught of new and changing regulations and increased enforcement around them. There are many challenges here: ownership and evaluation of changing regulations, and creating a solution that does not operate in isolation are just two examples where risk tooling can help.

In summary, using IT to enable risk management can bring benefits in every area from compliance and regulation to standardization and predictive analytics, turning an organization's risk management activities from a business necessity to a business enabler. While risk tooling can help, it can never be the sole answer. The biggest challenge organizations face in improving their risk management with technology and risk analytics is in bringing all the different stakeholders together to build an integrated system. Operations need to take a holistic approach when looking at using technology and analytics to improve risk management. This is a journey which needs the involvement of all stakeholders, through the whole organization. The ultimate goal should be to utilize technology to embed effective risk management across the business and across all three lines of defense.

**Using IT to enable risk management can bring benefits in every area from compliance and regulation to standardization and predictive analytics, turning an organization's risk management activities from a business necessity to a business enabler.**



# MEDIA-REPORTED EVENTS: DATA ANALYTICS

## Search methodology

We used KPMG in the UK's *Astrus* infrastructure to scan the Internet for publicly available English news articles related to IT incidents. *Astrus* utilized LexisNexis as the primary data source and included some subscription-only news sources.

The Internet search methodology was built on the principle — “an IT (adjective) incident (noun) happened (verb)”. By applying this principle, we developed hundreds of combinations which were translated into queries and supplied to *Astrus* to retrieve relevant news articles and events.

We defined an IT incident as an event that affected the Availability, Quality or Security of Information or Technology.

The script was executed for the 12-month period from 1 September 2013 to 31 August 2014. More than 10,000 news articles were retrieved.

## Result set and analysis

The result set was analyzed using a combination of automated and manual techniques to improve accuracy and relevance so that:

- The result set included incidents rather than potential threats.
- The result set included incidents that happened during the time period rather than after effects (of a prior incident) that were reported during the time period.
- Each article in the result set represented one incident. If a news article included multiple incidents, then each was considered separately. If multiple news articles referred to the same incident, one of the articles was included in the analysis.

A total of 522 relevant IT incidents were included as part of the final result set. Based on a pre-defined taxonomy, our IT risk professionals then reviewed these incidents and identified the following attributes for each incident.

- What happened?
- What were the causes?
- Affected companies and industries
- What was the estimated financial impact?
- How many entities or people were known to be affected?

The resulting analysis was presented to our technology risk specialists to draw judgements and conclusions which have been presented earlier in this report.

*The Internet search methodology was built on the principle — “an IT (adjective) incident (noun) happened (verb)”*

*Astrus, KPMG's secure on-line due diligence tool, provides a robust and cost-efficient way to obtain information and assess risks associated with customers, agents and counterparties. Astrus uses advanced search technologies to scour an extensive range of on-line public data sources, global sanctions and regulatory enforcement lists, corporate records, court filings, and press and media archives.*

*For further information on Astrus, please visit the KPMG website at <http://www.kpmg.com/uk/en/services/advisory/risk-consulting/services/forensic/pages/astrus-enhanced-due-diligence-and-astrus-monitoring.aspx>.*



# CONTACT US

## A - Z



**Daniel Gorton**  
KPMG in the UK  
daniel.gorton@kpmg.co.uk



**Jon Dowie**  
KPMG in the UK  
jon.dowie@kpmg.co.uk



**Ronald Plesco**  
KPMG in the US  
rplesco@kpmg.com



**David DiCristofaro**  
KPMG in the US  
ddcristofaro@kpmg.com



**Kiran Nagaraj**  
KPMG in the UK  
kiran.nagaraj@kpmg.co.uk



**Stephen Bonner**  
KPMG in the UK  
stephen.bonner@kpmg.co.uk



**Greg Bell**  
KPMG in the US  
rgregbell@kpmg.com



**Martin Lunt**  
KPMG in the UK  
martin.lunt@kpmg.co.uk



**Tony Torchia**  
KPMG in the US  
atorchia@kpmg.com



**John Machin**  
KPMG in the UK  
john.machin@kpmg.co.uk



**Michael Elysee**  
KPMG in the UK  
michael.elysee@kpmg.co.uk



**Vivek Mehta**  
KPMG in the US  
vivekmehta@kpmg.com



**John White**  
KPMG in the UK  
john.white@kpmg.co.uk



**Phil Lageschulte**  
KPMG in the US  
pjlageschulte@kpmg.com



Some or all of the services described herein may not be permissible for KPMG Audit clients and their affiliates.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2014 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. Printed in the U.S.A.

The KPMG name, logo and “cutting through complexity” are registered trademarks or trademarks of KPMG International.

Oliver for KPMG | OM023396A | November 2014.