Deloitte.

Foundations in a technology driven world

2016 EMEA Financial Services IT Risk Management Survey

At the core of every financial institution is a technology company

Overview

Foreword

Technology enables processes to operate efficiently and effectively, running 24 x7 without error. It supports employees in performing their day jobs quicker, and it is increasingly a fundamental part of overall business strategy as emerging and disruptive technologies offer new markets and ways to increase existing market share.

As technology becomes more pervasive, so do the associated risks; failing to manage these risks creates front page news, as well as an unwelcome and often material financial, customer and reputational impact. Regulators are responding accordingly, with many EMEA regulators paying particular attention to the risks associated with technology (for example, the FCA in the UK included 'Innovation & Technology' as a key priority in their 2016/17 business plan).

Our Objectives

This report has been written to help senior management and those in risk management, governance and oversight roles to better understand the key IT risk challenges facing peers across the Financial Services industry, as well as to provide our view on some of the drivers and priority actions needed to address them.

EMEA Insights

In developing the report, we surveyed IT Risk professionals across EMEA to comment on the key risks, issues and challenges they face in managing IT risk. Our survey included respondents from across the three lines of defence, including IT senior management, first line IT risk functions, second line IT risk functions, and IT internal audit. This gives a unique insight into the differing perspectives across these groups, as well as areas of commonality.

Results

Across the Financial Services industry we have seen evidence of an underinvestment in people, processes and supporting systems, coupled with an ever increasing reliance on technology to achieve business strategy and exposure to increasingly complex risks, such as cybercrime. This creates an extremely challenging environment in which to manage IT risks efficiently, effectively and in a way that adds value to the business.

We hope this report provides you with a useful insight into some of these challenges, as well as a view of the opportunities that more robust IT risk management practices will provide.

Our key findings

Driving board level focus

Strategic importance of managing technology risk

Our findings indicate that the strategic importance of managing technology risk has never been higher. The consequences of getting it wrong severely impact an organisation's reputation, customer confidence and loyalty, driving IT risk management firmly up the board agenda.

As we look ahead, governance of 'mission critical programmes' will be key as IT shoulders an increasingly burdensome change portfolio to support business strategy.

IT Risk operating models

Adapting to change

With the Business, IT and Operational Risk functions all in the process of re-evaluating their own operating models, the IT Risk function itself has had to adjust too. Our survey indicates that many organisations are struggling with the same fundamental questions – how to position the IT Risk function as a 'value creator' rather than a cost centre and how to enhance the three lines of defence model to better serve key stakeholders.

The evolving risk landscape

Prioritising focus

Emerging risks around change execution and operational resilience have joined cybercrime, data security, and third party management as being the most pressing IT risks identified by our respondents. The survey also identified differences in the responses between those in 'risk management' roles in the first line of defence and those in 'risk governance and oversight' roles in the second and third lines of defence.

Are organisations in control?

Divergence between risk exposure and risk appetite

Our suvey indicates a gap between business risk exposure - which is growing due to the increased strategic and operational dependence on IT - and business risk appetite, which is not increasing at the same pace. Respondents also identified with a common challenge around accurately measuring business risk appetite.

The talent conundrum

Recruit, train or buy?

With the rapid pace of change across Financial Services, having individuals with the right blend of IT, risk and business experience is often the key to being able to respond to the evolving needs of the business. As IT Risk functions compete to attract the best talent, those without a focused talent strategy are struggling to keep up, resulting in an inability to deliver real value to the business and focussing on risk adminstration rather than true risk management.

Driving board level focus

Our findings indicate that the strategic importance of managing technology risk has never been higher. The consequences of getting it wrong severely impact an organisation's reputation, customer confidence and loyalty, driving IT risk management firmly up the board agenda.

Focus on the here and now

Technology is seen as a critical business enabler for driving growth, margin, and efficiency, but it also presents a pervasive risk that must be understood and managed. Unsurprisingly, our respondents recognised that executive attention on IT risk management is ever increasing. Compliance with new and existing regulation was a clear leader in terms of focus with over 85% indicating it was one of the top two priorities for their executive. Many organisations still do not feel fully equipped to respond to the regulatory challenge, especially those with a global and multi-product footprint.

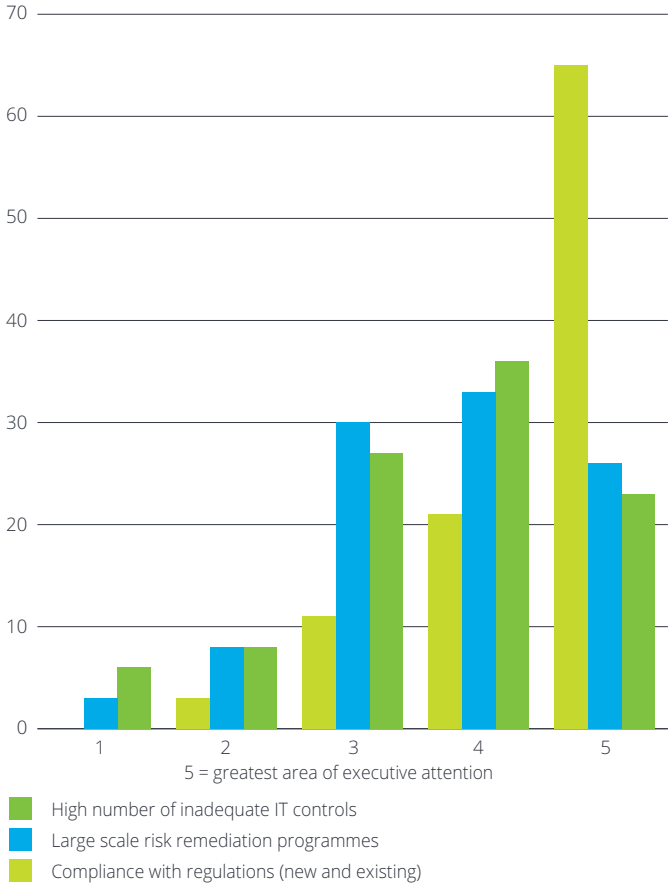
Our findings also indicate an increased focus from the executive on large scale remediation programmes. These programmes are typically commissioned to address hotspots and demonstrate step change improvements in the control environment. They often trigger intensive tactical effort and create significant executive attention.

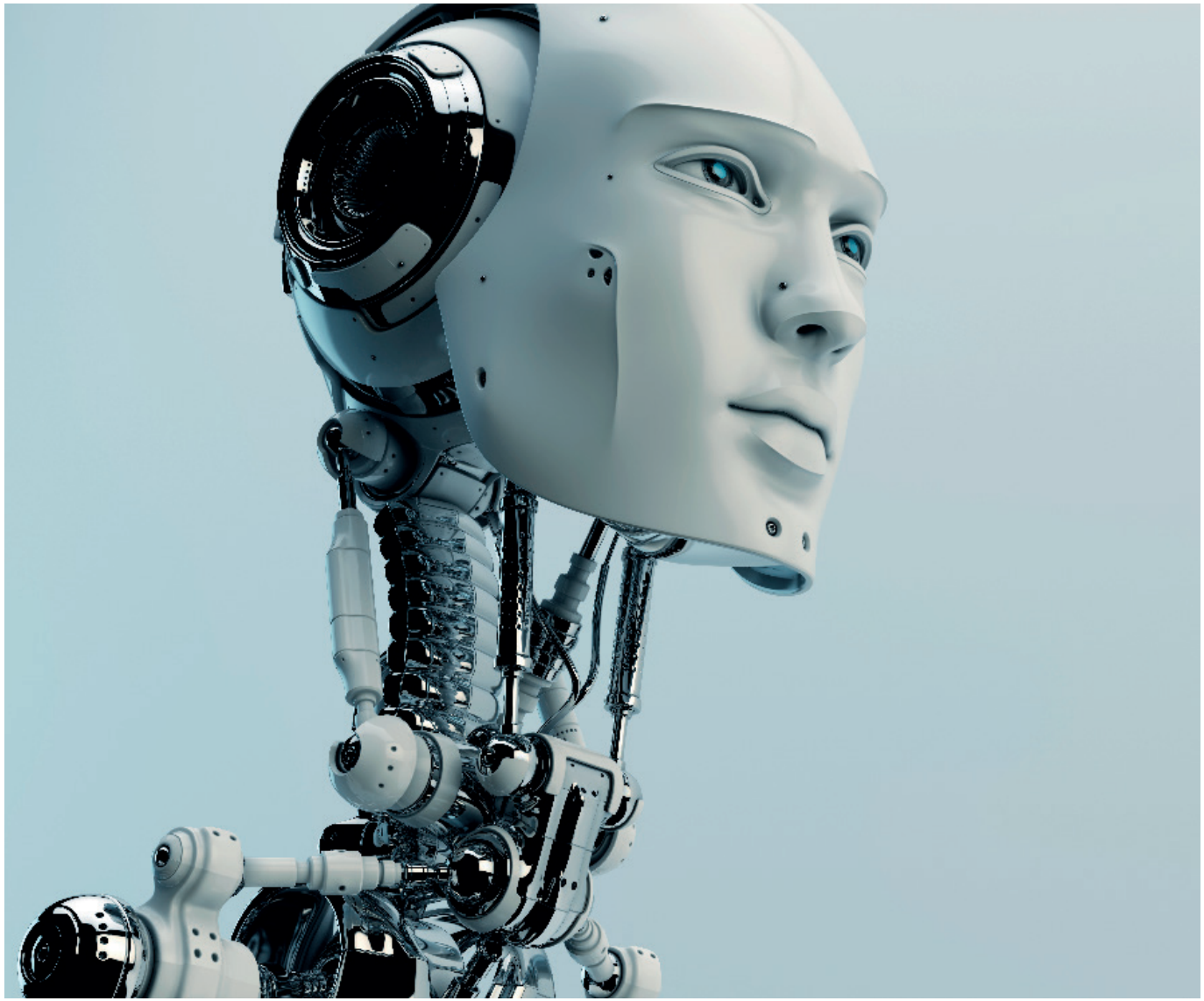
Yet, whilst such programmes have their place, there is often a tendency to focus on short term improvements, layering 'controls on controls' rather than prioritising more strategic activities (such as cultural change, control automation and delayering) to help embed a self-sustaining environment that can address hotspots through business as usual continuous improvement. As such, these programmes can often struggle to show a direct linkage between what they have delivered and real risk reduction, particularly when measured through established business as usual methods such as key risk indicators.

OVER 85%

Compliance with new and existing regulation was a clear leader in terms of focus with over 85% indicating this was one of the top two priorities for their executive

Top 3 areas of executive attention reported by our respondents





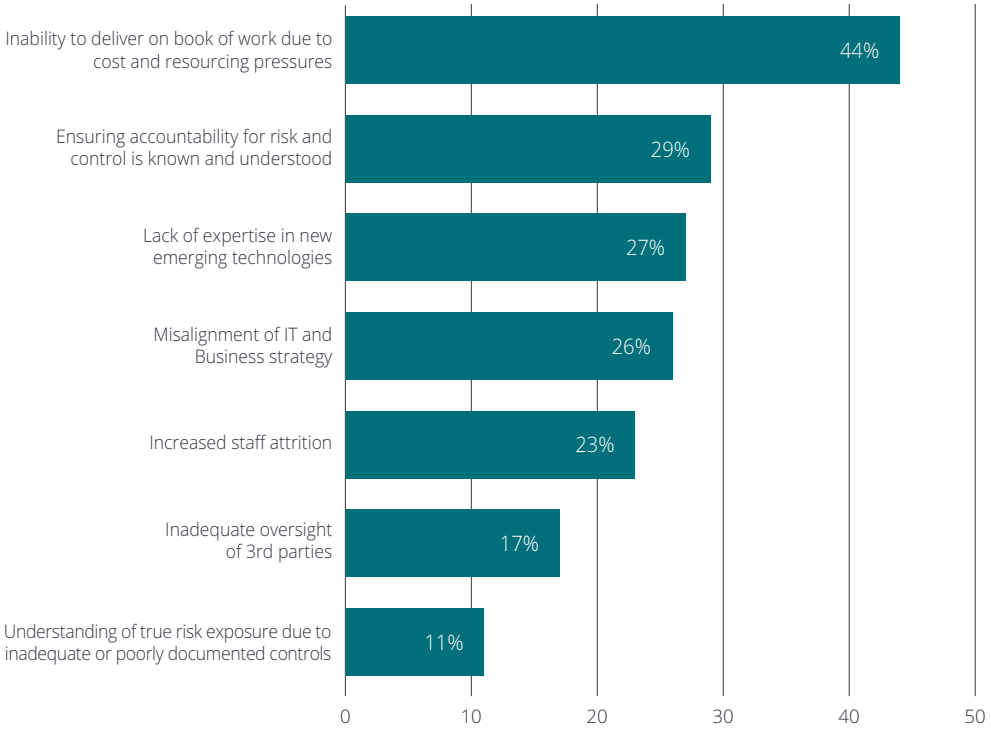
An eye on the future

As we look ahead, governance of 'mission critical programmes' will be key as IT shoulders an increasingly burdensome change portfolio to support business strategy.

27% of respondents saw not keeping abreast of emerging and disruptive technology as one of the greatest risks for IT. Our survey indicates that smaller organisations see this as their biggest risk, whilst larger retail and investment banks are more comfortable, as many now have dedicated functions to build and react to emerging technologies. Regulators are also focussing on this, for example the FCA in the UK have recently established a regulatory sandbox as a means for businesses to 'test' their innovative products, services, business models and delivery mechanisms.

Closely related are respondent's views that aligning business and IT strategy will become a key risk in the future. Our experience shows that this is especially prevalent in those organisations where senior management focus is on the 'more, quicker' approach, when IT are focussed on 'keeping the lights on' for legacy systems and infrastructure. This divergence can not only create further strain on resources, but also have unintended consequences on the IT environment.

Top risks faced by the IT function in the future



Percentage of respondents that reported this risk as one of their top three or similar.

45% of respondents see failing to keep up with the pace of business change as one of the greatest future risks faced by the IT function

Deloitte point of view

The ever increasing attention on IT risk from the Board is proportionate, but there is a perception across our respondents that this attention is predominantly focussed on reacting to the 'here and now'.

Given the pace of technological change, the Board should ensure sufficient attention is paid to 'forward looking' execution risk (i.e. the ability to deliver on an ever increasing order book against a backdrop of strategic change), as well as the threats and opportunities posed by emerging disruptive technologies.

As the strategic importance of IT increases, the execution risk to the wider organisation becomes very real. This risk can be compounded by management decision making that often has unintended consequences on the cost and complexity of the IT environment. Those in governance and oversight roles should ensure that organisations are equipping themselves with the tools, techniques and resources to reduce this execution risk.

Organisations that do this well tend to have a close alignment between IT Risk functions and the wider business risk teams, getting on the front foot in understanding new technologies and business strategy, and ensuring they play a closer role in business decision making, in real time.

They also tend to invest in delayering and automation of the IT control environment – simplifying the landscape and building automated controls into business processes to support risk based proactive decision making.

IT Risk operating models

Adapting to change

With the Business, IT and Operational Risk functions all in the process of re-evaluating their own operating models, the IT Risk function itself has had to adjust too. Our survey indicates that many organisations are struggling with the same fundamental questions – how to position the IT Risk function as a 'value creator' rather than a cost centre and how to enhance the three lines of defence model to better serve key stakeholders.

Adapting to wider operating model changes

Our survey shows that 47% of respondents in the first and second lines say their function has gone through significant organisational change in the last 12 months, with a formal split of the first and second lines being the most common theme emerging – 70% say they now have separate first and second line risk teams. However, with 75% of respondents saying a clear division of responsibilities between the first line of defence and the second still does not exist, this is a clear indication that organisations must dedicate further time and effort to embedding change so that staff, and the wider organisation, understand the new split of responsibilities.

75% of respondents say they do not have a clear division of responsibilities between the first and second line of defence

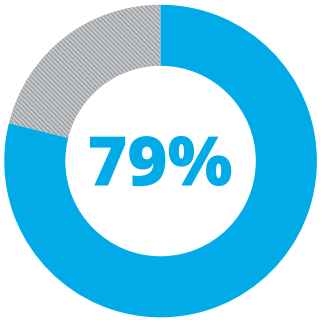
Without clarity on each others remit, the inevitable outcome is confusion on respective roles between both teams, and this can lead to overlap, friction, and gaps - only 7% of first and second line respondents see their counterparts in the other line of defence as a 'trusted partner adding value'. This will need to change if the three lines of defence model is to achieve what it is designed to do in an efficient and effective way.

Structural differences across the lines of defence

Our survey shows that second line IT Risk teams have more of an emphasis on a regional structure than first line teams, which are predominantly functionally aligned. Whilst both structures have their merits, awareness of this difference in structure, and the day to day challenges it creates, is key to embedding a successful interaction model between the two lines of defence.

Using the IT risk operating model to embed accountability

Clear accountability for risk and control should be a natural outcome of an IT risk operating model that is fully embedded. As referenced elsewhere in this report, 79% of respondents say that 'ensuring accountability for risk and control is known and understood' will be a key risk for the IT function over the next 12 months. Until IT risk operating models are fully embedded, efforts to embed accountability are unlikely to be successful or sustainable.



of respondents believe ensuring accountability for risk and control will be a top 5 risk over the next 12 months

Only 7% of respondents see their counterpart in the first or second line of defence as a trusted partner

of respondents said their offshore IT Risk team was larger than their onshore IT Risk team

Leveraging offshore resourcing models

With pressure mounting to increase output whilst minimising cost, and the pressing need to transition from 'reactive risk administration' to 'proactive risk management', many organisations are assessing how they can use offshore models to gain access to technical experts at a lower price point and centralise 'repeatable and high volume' administrative tasks offshore. Our survey results give examples of 'early adopters' who already have a greater presence offshore than onshore.

Deloitte point of view

We expect to see further integration of IT Risk teams with other related risk disciplines, with combined teams being able to improve resiliency by redefining and responding to the risk scenarios that underpin traditional IT risk frameworks. In order to do this they will need to leverage a consistent set of optimised risk management services across Group functions, not just IT.

Many of our clients tell us that whilst the three lines of defence model makes sense on paper, the detailed guidance required to implement it successfully is lacking. This has led to senior management time being spent on resolving day to day challenges, eroding the value provided by the IT Risk function to IT and the wider organisation.

In our view, there are five areas IT Risk functions should look at when improving their value proposition:

- Driving a clear and succinct accountability model to show what is performed in each line of defence and, critically, what are the accountabilities of front line risk and control owners
- Using data analytics and metrics to challenge the first line on how they are identifying and managing emerging risks
- Developing an internal thought leadership capability that allows the function to act as an advisor to the business on the risks posed by emerging technologies and other advances, such as automation and robotics
- Re-thinking the nature of their involvement in governance and oversight activities to bring more value to the table
- With 53% of respondents rating a 'Loss of operational capability due to a lack of a sufficient organisational resilience capability' as a top 5 risk, the increased regulatory focus on 'organisational resilience' is justified.

The evolving risk landscape

Prioritising focus

Emerging risks around change execution and operational resilience have joined cybercrime, data security, and third party management as being the most pressing IT risks identified by our respondents. The survey also identified differences in the responses from those in 'risk management' roles in the first line of defence and those in 'risk governance and oversight' roles in the second and third lines of defence.

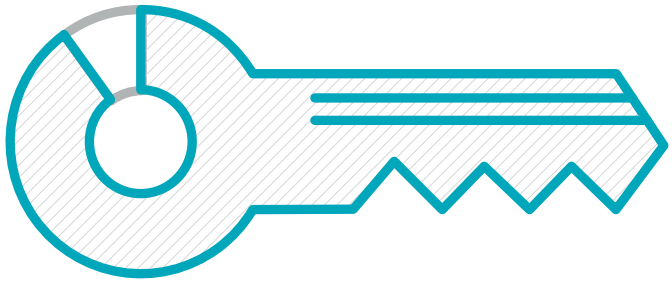
Vulnerability to external threats (including hacking and cyber crime)

With cyber security being pushed to the top of the board agenda, it comes as no surprise that it is perceived as the top risk, with 90% of our respondents including it as one of the top five risks facing their organisation. This sentiment was echoed across all lines of defence, which is understandable given the added pressure on all lines to identify external threats and ensure that appropriate control procedures are implemented to mitigate the risk.

90% of organisations perceive cyber security as one of their top five IT risks

Loss of sensitive client or proprietary data

As financial institutions become increasingly dependent on complex environments that use both internal and external data feeds, the risks posed by inadequate data security controls increase. 60% of our respondents saw this as one of the top five risks facing their organisation. Our second line of defence respondents saw this as a lower risk (6) than other respondents.



Top IT risks

Comparison of top IT risks reported by respondents in our 2016 survey compared to those in our previous survey run in 2013.

	2016 ranking	2013 ranking
Vulnerability to external threats (incl. hacking, cyber crime)	1st	Joint 2nd
Loss of sensitive client or proprietary data	2nd	Joint 2nd
Inability of the IT function to keep up with the pace of change required	3rd	New Entry
Inadequate oversight of third parties	4th	1st
Loss of operational capability due to a lack of a sufficient organisational resilience capability	5th	4th

Breakdown of top 5 IT risk by line of defence (2016 ranking only)

	1st line of defence	2nd line of defence	3rd line of defence	Overall
Vulnerability to external threats (including: hacking, cyber crime)	1st	1st	1st	1st
Loss of sensitive client or proprietary data	2nd	6th	3rd	2nd
Inability of the IT function to keep up with the pace of change required	7th	4th	2nd	3rd
Inadequate oversight of third parties	3rd	3rd	4th	4th
Loss of operational capability due to a lack of a sufficient organisational resilience	4th	2nd	7th	5th

Inability of the IT function to keep up with the pace of change required

This IT risk featured prominently in our survey responses this year, which is reflective of the heightened execution risk covered elsewhere in this report. Our experience shows that the first lines of defence are often hit hardest by the sheer volume of change, but it is those that are charged with risk governance and oversight (second and third line) that have identified this as a key IT risk in our survey.

Inadequate oversight of third parties

As third party relationships within financial services continue to proliferate, so do the associated risks. Often effective third party management can be obscured by vanilla forms of vendor assurance or check-box due diligence. With this in mind it is unsurprising that 59% of our respondents stated that it is in the top five IT risks facing their organisation. 47% of respondents stated that their organisations were reliant on third parties, which suggests that this should continue to be a key focus area for organisations.

59%

of respondents indicate third party risk management is one of their top five IT risks

Loss of operational capability due to a lack of sufficient organisational resilience capability

With technology enabling virtually every activity within financial services, technology resilience is paramount to preventing disruptions and outages. This was acknowledged by 53% of our respondents who saw this as one of the top five IT risks facing their organisation. Institutions need a transparent end-to-end view of all technology required to support particular products in order to perform comprehensive resilience testing, as often technology components are only tested in isolation which does not provide assurance across the overall resiliency of the product.

Deloitte point of view

Effective and efficient risk identification is critical to ensuring that resource and attention is prioritised in the right places. This is often made challenging by the complexity and scale of many financial services organisations. Whilst there is a degree of alignment across the three lines of defence, we have still identified a number of interesting anomalies. These illustrate the need for first and second line IT Risk teams to work closer together to build consensus on the most pressing risks facing their organisation.

In many ways though, risk identification is just the tip of the iceberg – IT risk is often the risk that the typical Board member may be the least well equipped or informed to understand and oversee. For example, there may be a relatively narrow view of IT risk taken by the Board (e.g. cyber, system availability), rather than a holistic appreciation of other IT risk areas such as change management, risks posed by automation, and underpinning factors such as execution risk.

Metrics and KRIs can be established to effectively monitor risks, not only demonstrating the risk exposure to the organisation, but also to demonstrate the effectiveness of risk mitgation techniques and initiatives.

Are organisations in control?

The divergence between risk exposure and risk appetite

Our suvey indicates a gap between business risk exposure - which is growing due to the increased strategic and operational dependence on IT - and business risk appetite, which is not increasing at the same pace. Respondents also identified with a common challenge arround accurately measuring business risk appetite.

Over 60% of respondents felt their IT risk exposure had increased over the past 12 months, 30% of which said that this increase has been 'significant'.

Survey respondent views on the causes of increased risk exposure

- Increased automation and dependence on IT
- Exposure to cyber risks
- Disruptive technology entrants
- Evolving technology demands
- Implementation of new platforms and technologies
- Business changes and new markets

Conversely, only 24% of our respondents indicated that their organisation's risk appetite had increased during this period. Where risk appetite had increased, often this was due to cost pressures and business strategy changes, necessitating a fresh perspective on what is within tolerance.

Over 60%

of respondents feel their exposure to IT risk has increased over the past 12 months

Deloitte point of view

The significant increase in risk exposure demonstrates how critical effective IT risk management is to an organisation.

It is key that organisations review their internal and external risk exposure on a regular basis, but also that they then review their risk appetite at a granular level for each area of IT risk.

This granular review will help prioritise resources and budget, as well as support the business to take informed decisions on strategy.

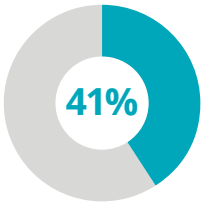
Risk appetite may increase for a number of valid reasons, so it is important that a common view is held across the organisation so that informed decisions can be made. Defining a consistent set of risk indicators (KRIs), metrics and thresholds provides an objective assessment as to whether IT risk is within appetite. Ensuring there are leading and lagging indicators in the population will support in establishing proactive risk management capabilities, enabling corrective actions to be instigated before risks materialise into issues.

An effective and robust dispensation and waiver process is crucial to avoid the creation of a pseudo risk appetite and false assurance of operating within appetite. Due to the associated potential impact on capital management plans, care should be taken to increase IT risk appetite solely on cost grounds and without following due governance processes.

The Talent Conundrum

Recruit, train or buy?

With the rapid pace of change across Financial Services, having individuals with the right blend of IT, risk and business experience is often the key to being able to respond to the evolving needs of the business. As IT Risk functions compete to attract the best talent, those without a focused Talent strategy are struggling to keep up, often acting as 'risk administration' functions rather than true 'risk management' functions.



of respondents ranked 'People and Skill' as the top challenge in managing IT Risk over the next 12 months

The challenges of finding and hiring the right talent

With the broad range of experience required to manage IT risk effectively, it is no surprise that 71% of respondents indicate that finding suitable candidates in the market is a struggle. 46% of respondents say they have open head count (70% for the first line of defence). 61% cite a lack of relevant technical risk and controls knowledge as the most common reason for candidates being unsuccessful at interview (100% for the first line of defence). Our survey further indicates that there is a war for talent with competitors, with only 22% of respondents saying they recruit from outside Financial Services.

When looking at career experience, there is a clear distinction between those in the first line, whose background tends to be more in operational IT rather than risk and control, and those in the second and third line whose background tends to be in IT risk and IT audit, but not necessarily operational IT. Re-thinking traditional recruitment channels and career paths may be the answer to solving this imbalance in the long term by producing candidates who have both operational IT and risk and control experience in equal measure.

Our survey shows that most organisations do not currently recruit directly from the graduate market. Whilst not a short term fix, this is an untapped opportunity for organisations to build their own talent pipeline, reduce their dependency on external hires and formalise approaches to succession planning.

70% of respondents in first line risk teams have previously held a role within IT, compared to 25% of second line respondents and 20% of third line respondents

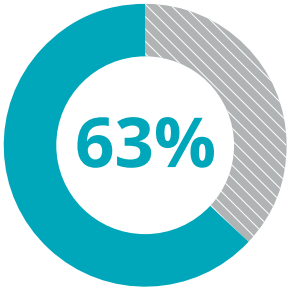
Only **9%** of respondents in IT, and 40% of respondents in first line risk teams, have previously held an audit role

Investing in training and development and monitoring ROI with the right metrics

Given the ongoing war for talent and the proliferation of new technology solutions coming to market, the retention and development of key staff is vital to maintain and continually improve service levels to the business.

Where skills gaps exist, it can be more efficient to train, rather than hire, but 63% of respondents said there is no formal risk and control training programme in place at their organisation. This can lead to staff being asked to perform activities outside of their skillset, reducing the opportunity for them to add value and drive quality. It can also lead to a 'blurring of the lines' between first and second line IT Risk teams as people go in search of the right skillsets, irrespective of which line of defence the individual with the right skills sits in.

In the current cost conscious climate, any investment in training will require a strong business case and a robust way of measuring return on investment. This data can be driven from performance appraisals, although the majority of respondents (54%) indicated that their organisation does not include risk and control metrics in performance appraisals.



of respondents have no formal risk and control training programmes in place

Filling 'niche' skillset gaps with the right temporary resource

47% of respondents said they are 'partially' or 'very' reliant on third parties. With such a deep level of technical expertise required across such a broad range of subjects, and spikes in demand for services throughout the year, this can be a useful resourcing strategy, though ensuring continuity is retained in-house is important to retain 'corporate memory' and reduce reliance on temporary resource.

Deloitte point of view

The increased level of scrutiny on spend is pushing the IT Risk function along the maturity curve, and we are seeing a wave of transformation programmes to create leaner, more effective and more proactive IT Risk functions that are closely integrated with other risk disciplines.

The IT Risk function has developed organically over the last 10 years and now needs to think more strategically about its people. Without a pipeline of talent to deliver over the long term Risk functions will lag behind their organisation in developing the right skills, knowledge and market exposure to effectively manage risk. It is critical that organisations do not fall foul of the 'corporate memory' gap, where third parties are relied on within business as usual roles to provide skills, services and continuity that does not exist in house.

A clear talent strategy is needed to attract the right graduates, to provide opportunities to gain both IT and risk and control experience in equal measure and to create a career path for top performers to reach the top. Closer collaboration across the lines of defence on key performance metrics is needed to ensure everyone is pulling in the right direction. These metrics will need careful design to avoid driving behaviour that is reactive rather than proactive, or driving silo behaviour to the detriment of embedding an effective three lines of defence model.

Control automation, a greater use of data analytics and the trend for activities such as independent controls assurance to be delivered by lower-cost utilities will allow a greater proportion of time spent by first line FTE to be spent on value add initiatives and which both supports the attraction and retention of talent, and improves value for the business.

In order to deliver on the wave of transformation initiatives the IT Risk talent agenda needs to evolve, and quickly.

Key Contacts

Financial Services IT Risk Management

Chris Recchia
Partner
Risk Advisory
+44 7795 667595
crecchia@deloitte.co.uk

Rob Dighton
Senior Manager
Risk Advisory
+44 7717 541579
rdighton@deloitte.co.uk

Tom Bigham
Director
Risk Advisory
+44 7917 084327
tbigham@deloitte.co.uk

Matt Entwistle
Senior Manager
Risk Advisory
+44 7827 958443
mentwistle@deloitte.co.uk

Deloitte.

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

Designed and produced by The Creative Studio at Deloitte, London. J8645