## Contents

- Foreword .................................................. 01
- About the survey ........................................ 02
- The business impact of disruptive technology .... 04
- Governance of digital transformation ............... 11
- Areas of emerging risk as a result of digital transformation ........................................ 16
- The operating model for risk .......................... 22
- Use of disruptive technology to manage risk digitally .................................................. 28
- Talent ........................................................... 33
- Authors and Contributors ............................... 38
- Global contacts ............................................. 39
- Notes ........................................................... 40
Foreword

I am delighted to share with you our first Global Digital Risk Survey. Most of the 160+ organisations we interviewed are going through some degree of digitisation or indeed digital transformation. They talked to us candidly about their digital aspirations, ranging from building entirely new business models to creating more personalised products and services empowered by artificial intelligence (AI), big data and cloud. They also shared the significant challenges they are facing with the pace of change, cultural adoption, the cyber threat, the scarcity of skilled resources and regulatory compliance. We hope you find the content stimulating and helpful in your own digital journey and we look forward to hearing your views on the key issues highlighted by the survey.

Overview

Whilst it takes many years to build up customer loyalty, this trust can be lost overnight in a digital world and organisations must find a way to maintain control as they transform for the digital era. This report, which presents the results of our 2019 Global Digital Risk Survey, provides global perspectives on the opportunities and challenges that the adoption of disruptive technology bring to managing risk and provides our latest thinking on how to overcome some of those challenges.

Our aim is to shine a light on what is happening ‘on the ground’ with the adoption of emerging technology, and highlight the role that effective management of risk can play in helping organisations deliver their digital strategy. The common theme throughout this report is therefore one of maximising the commercial opportunity presented by the digital economy. Strong leadership, clear ownership and effective action will help to accelerate this journey.

We would like to thank our clients around the world who took part in this survey for the openness in which they shared their perspectives and challenges, many of which are similar across regions and industries.

Stephen Ley
Global Lead Partner, Technology and Digital Risk

Report structure

1. The business impact of disruptive technology – to what extent are organisations adopting disruptive technology, how quickly are they able to deploy it and what barriers to adoption exist?
2. Governance of digital transformation – do organisations feel confident that they are adequately controlling the adoption of disruptive technologies, and how confident are they that their governance approach is fit for purpose and scalable?
3. Areas of emerging risk as a result of digital transformation – what risk themes are emerging as the speed and extent of digital transformation increases? How much focus is being placed on them?
4. The operating model for Risk – what implications is the adoption of disruptive technology having on approaches to risk management activities?
5. Use of disruptive technology to manage risk – are organisations leveraging disruptive technology in order to manage risk at the speed and scale now required?
6. Talent – what skillsets are organisations looking for in order to respond to the challenges of managing digital risk?
About the survey

Overview
This survey gauges the sentiment that senior executives across the three lines of defence have towards disruptive technology and its impact on their organisation. We surveyed 166 individuals from organisations across EMEA, the Americas and Asia Pacific, sitting across Digital, Transformation, Technology, Risk and Internal Audit functions. Participating organisations operate in sectors such as financial services, consumer products and retail, telecoms, health and life sciences, oil and gas and technology.

Methodology
This survey was commissioned by Deloitte LLP and conducted between December 2018 and March 2019.

Our team of researchers either directly interviewed survey participants or engaged them through an online survey.

Our field research was then analysed by in-house industry and subject matter experts to identify common themes, key lessons and questions for further consideration.

Demographics

Figure 1. Demographic split of survey respondents

Line of defence

- 1st line of defence – non risk role: 28%
- 1st line of defence – risk role: 24%
- 2nd line of defence: 33%
- 3rd line of defence: 15%

Regional split
- EMEA: 55%
- Americas: 29%
- APAC: 16%

Industry split

- Financial Services
- Consumer Products 
  & Retail
- Telecoms
- Manufacturing
- Health
- Oil and Gas
- Other
- IT
- Other
The business impact of disruptive technology
The business impact of disruptive technology

A once in a generation opportunity awaits for those able to overcome the barriers

In many ways, technology is now allowing businesses to do what they have always wanted to do by making the previously impossible, possible. The irony now is that many of the barriers to achieving true digital transformation are no longer technology related, but related to culture, skillset, execution capability and ability to manage risk. A combination of these attributes are required to decide on, and clearly articulate, the business case for further adoption – something many organisations appear to still be coming to terms with.

Opportunities galore, but significant barriers stand in the way

Opinions converge across all regions, industries and functions – disruptive technologies have the potential to create huge value for organisations. From a faster time to market, to getting to know your consumers better, to the creation of new product categories with global scale, survey respondents suggest new business models can unlock huge commercial value. But such opportunities do not come without obstacles. The barriers to digital transformation highlighted by respondents vary – from legacy processes to cultural resistance, lack of talent and capability to aged infrastructure.

What is having the biggest impact right now?

Our survey shows that when it comes to overall adoption trends, cloud (85%), agile development (80%), agile delivery (77%) and application programming interfaces (APIs) (76%) are leading the way. Large scale adoption of many other emerging technologies appears to still be in its infancy, with ‘adoption at scale’ figures for the likes of Internet of things (IoT), robotics, machine learning, blockchain and natural language processing all below 10%. See Figure 2 for the full breakdown of adoption trends.

From a faster time to market, to getting to know your consumers better, to the creation of new product categories with global scale, survey respondents suggest new business models can unlock huge commercial value.

Opportunity for creating a digital advantage

Given the extent of current adoption levels and appetite for the adoption of cloud, agile and APIs, risk teams should be ensuring that governance approaches for each are embedded, well understood and capable of supporting further growth in adoption.
Beyond the hype – which trends are most widely adopted?

Figure 2. Breakdown of adoption trends by overall adoption level and type of use

The leaders – Established technologies and approaches such as cloud, agile and APIs have overall adoption levels of greater than 75% amongst survey participants. These four also have the highest ratings for ‘at scale’ and ‘adopted for customer use cases’.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Overall adoption</th>
<th>Top 3 barriers to scaling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud</td>
<td>85%</td>
<td>30% Risk appetite, 19% Maturity of governance model, 27% Regulatory scrutiny</td>
</tr>
<tr>
<td>Agile development</td>
<td>80%</td>
<td>28% Cultural resistance, 14% Maturity of governance model, 23% Lack of talent</td>
</tr>
<tr>
<td>Agile project</td>
<td>77%</td>
<td>23% Cultural resistance, 17% Maturity of governance model, 13% Lack of talent</td>
</tr>
<tr>
<td>APIs</td>
<td>76%</td>
<td>22% Lack of talent, 25% Difficulty in articulating the business case, 19% Lack of bandwidth</td>
</tr>
</tbody>
</table>

Top 3 barriers to scaling:
- Risk appetite
- Maturity of governance model
- Regulatory scrutiny
- Cultural resistance
- Maturity of governance model
- Lack of talent
- Difficulty in articulating the business case
- Maturity of capability
- Lack of talent
- Lack of talent
- Lack of bandwidth
- Difficulty in articulating the business case
- Maturity of capability
- Lack of talent
- Board acceptance/understanding

The chasing pack – Adoption of robotics and automation, machine learning and internet of things (IoT) are next in line with adoption levels between 50% and 75%. This group also have the highest level of experimentation with proof of concepts, demonstrating efforts to discover the most valuable uses of these technologies.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Overall adoption</th>
<th>Top 3 barriers to scaling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automation and Robotics</td>
<td>71%</td>
<td>4% Difficulty in articulating the business case, 13% Maturity of capability, 33% Budget constraints</td>
</tr>
<tr>
<td>Machine learning</td>
<td>60%</td>
<td>2% Difficulty in articulating the business case, 8% Maturity of capability, 8% Lack of talent</td>
</tr>
<tr>
<td>Internet of Things</td>
<td>54%</td>
<td>9% Difficulty in articulating the business case, 13% Maturity of capability, 12% Lack of talent</td>
</tr>
<tr>
<td>Natural language processing</td>
<td>50%</td>
<td>1% Difficulty in articulating the business case, 5% Maturity of capability, 5% Lack of talent</td>
</tr>
</tbody>
</table>

Top 3 barriers to scaling:
- Difficulty in articulating the business case
- Maturity of capability
- Lack of talent
- Difficulty in articulating the business case
- Maturity of capability
- Lack of talent
- Difficulty in articulating the business case
- Maturity of capability
- Lack of talent
- Difficulty in articulating the business case
- Maturity of capability
- Lack of talent

The future players – Other trends, such as microservices and blockchain, represent the lowest overall adoption figures from our survey. Experimentation far outweighs any other category for blockchain, where as microservices has a broadly equal split across each adoption category.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Overall adoption</th>
<th>Top 3 barriers to scaling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microservices</td>
<td>40%</td>
<td>8% Difficulty in articulating the business case, 10% Maturity of capability, 14% Lack of talent</td>
</tr>
<tr>
<td>Blockchain</td>
<td>34%</td>
<td>4% Difficulty in articulating the business case, 2% Maturity of capability, 23% Board acceptance/understanding</td>
</tr>
</tbody>
</table>

Top 3 barriers to scaling:
- Difficulty in articulating the business case
- Maturity of capability
- Lack of talent
- Difficulty in articulating the business case
- Maturity of capability
- Lack of talent
- Difficulty in articulating the business case
- Maturity of capability
- Lack of talent
- Difficulty in articulating the business case
- Maturity of capability
- Lack of talent

Key:
- Adopted at scale
- Adopted for customer use cases
- Adopted for internal use cases
- Experimenting
Which regions are leading the way?
Adoption levels in each region broadly mirror the global adoption trends, with cloud, agile development, agile delivery, and APIs featuring in the top four most widely adopted trends. Cloud came top of the list of technologies adopted at scale across APAC and the Americas, with agile development techniques most common in EMEA. The results point to the APAC region as the leader in adoption of cloud technology, with the percentage of organisations adopting the technology at scale nearly double that of the Americas (see Figure 3).

What are the most common barriers to scaling adoption?
Difficulty in articulating the business case (20%) was the most common barrier to scaling adoption (see Figure 4). With so many options now available, it appears that organisations are grappling with deciding on how best to apply new technologies to generate commercial value. Perhaps tellingly, the second and third most popular answers related to capability maturity and lack of talent, both of which play a large part in being able to articulate how technology can be applied.

The most common barriers to scaling adoption are not regulatory scrutiny, lack of senior support or board acceptance, but challenges in articulating the business case, talent, capability, governance model and culture.

Who and what is leading the way?
Figure 3. Percentage of respondents by region who have adopted disruptive technologies at scale

Barriers to scaling adoption
Figure 4. Difficulty in articulating the business case stated as the most common barrier to scaling technology adoption
How quickly are organisations able to convert ideas into live solutions?

The vast majority of organisations (69%) reported that they are struggling to take ideas to market in under six months (see Figure 5). Although this varies slightly between regions, with the Americas and APAC regions reporting quicker times taken to deploy along with Manufacturing and IT when looking by industry. However on the whole, the results indicate there are no significant differences across geography or industry, which implies many are struggling with the same challenge - how to decrease ‘time to value’ whilst still maintaining control.

For organisations that take six months or more to convert ideas into live solution the obstacles are primarily around culture (e.g. such as a more conservative, waterfall approach to funding allocation), legacy processes (e.g. manual environment provisioning) and lack of talent. For organisations that are able to deploy quicker, culture and legacy processes are less of an issue but lack of talent remains as the biggest obstacle to going even quicker (see Figure 6 for the full breakdown).

Regardless of deployment time, the results highlight significant opportunity for risk teams to play their part in reducing the time, and cost, of delivering change. Resolving underlying issues with delays due to risk and control requirements, security requirements, culture, and agile teams having to interact with non agile teams all provide improvement opportunities to explore.

Just over one third of respondents (36%) report experiencing significant incidents due to disruptive technologies going wrong. Of that group, many saw more significant impact, lower frequency incidents arising from technologies further down the adoption curve (automation, blockchain) and lower impact higher frequency incidents with technologies being used currently (Cloud, APIs).

Whilst there will be outliers to this observation, it demonstrates how the risk profile of disruptive technologies varies along the adoption curve. As adoption grows, the likelihood for service disruption increases, demonstrating the need for governance approaches to be scaled up in line with adoption.

Most require six months to over one year to imagine and deliver a new solution. This phenomenon is almost uniform among industries and regions.
The value creation opportunity for risk management teams - helping the organisation decrease time to value

Figure 6 – The biggest obstacles impacting the time taken to convert ideas to live solutions, split by average time taken to convert ideas

Can convert ideas to solutions in under 6 months

<table>
<thead>
<tr>
<th>Obstacle</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delays due to security requirements</td>
<td>18%</td>
</tr>
<tr>
<td>Delays due to risk and control requirements</td>
<td>46%</td>
</tr>
<tr>
<td>Lack of automation</td>
<td>14%</td>
</tr>
<tr>
<td>Organisational culture</td>
<td>34%</td>
</tr>
<tr>
<td>Stakeholder understanding</td>
<td>41%</td>
</tr>
<tr>
<td>Legacy processes</td>
<td>45%</td>
</tr>
<tr>
<td>Lack of resource with the right skillset</td>
<td>64%</td>
</tr>
<tr>
<td>Delays caused by agile teams interacting with non agile teams</td>
<td>36%</td>
</tr>
</tbody>
</table>

Take 6-12 months

<table>
<thead>
<tr>
<th>Obstacle</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delays due to security requirements</td>
<td>15%</td>
</tr>
<tr>
<td>Delays due to risk and control requirements</td>
<td>32%</td>
</tr>
<tr>
<td>Lack of automation</td>
<td>17%</td>
</tr>
<tr>
<td>Organisational culture</td>
<td>53%</td>
</tr>
<tr>
<td>Stakeholder understanding</td>
<td>21%</td>
</tr>
<tr>
<td>Legacy processes</td>
<td>79%</td>
</tr>
<tr>
<td>Lack of resource with the right skillset</td>
<td>52%</td>
</tr>
<tr>
<td>Delays caused by agile teams interacting with non agile teams</td>
<td>21%</td>
</tr>
</tbody>
</table>

Take greater than 12 months

<table>
<thead>
<tr>
<th>Obstacle</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delays due to security requirements</td>
<td>10%</td>
</tr>
<tr>
<td>Delays due to risk and control requirements</td>
<td>27%</td>
</tr>
<tr>
<td>Lack of automation</td>
<td>17%</td>
</tr>
<tr>
<td>Organisational culture</td>
<td>65%</td>
</tr>
<tr>
<td>Stakeholder understanding</td>
<td>40%</td>
</tr>
<tr>
<td>Legacy processes</td>
<td>58%</td>
</tr>
<tr>
<td>Lack of resource with the right skillset</td>
<td>56%</td>
</tr>
<tr>
<td>Delays caused by agile teams interacting with non agile teams</td>
<td>15%</td>
</tr>
</tbody>
</table>
Plotting the way forward - where should organisations be focusing their efforts?

Due to the fast market dynamics of a digital environment, any barriers to achieving scale and speed can become strategic risks with a significant level of potential impact to the business. As a result, Risk functions have a significant role to play in helping organisations overcome these barriers by influencing the approaches taken to adopt new technologies quickly, but in a safe and secure manner.

• **Focus on the business need for transformation, not the technology** – in a world of such rapid technological change, it can be easy to focus primarily on the technology. However, the business need for transformation should be the primary driver. Once real business needs have been identified, focus should then be on the creation of well researched, compelling business cases and finding employees with the skillsets required to make them reality.

• **Understand and break through the barriers to speed** – the survey results suggest that legacy processes, skillset gaps, culture and approaches to addressing risk and control requirements are the primary factors impacting speed of change execution. Form a view of what the real issues are on the ground are that impact time to value and tackle them one by one.

• **Incorporate flexibility into governance frameworks and prioritise technologies that are relevant now** – business executives are unlikely to want to carry excessive risk unnecessarily, but they can’t afford for inefficient or overly rigid governance processes to get in the way either, or for them to limit innovation and risk taking. Governance and risk management becomes increasingly important as adoption grows and therefore a common methodology that allows for tailoring of approaches, whilst still remaining consistent with the common risk framework, should facilitate and encourage safe adoption.

Opportunity for creating a digital advantage

In a world where speed to market is critical, there is an opportunity for risk teams to create a real commercial advantage for their organisations by designing governance processes that reduce time to value.
Governance of digital transformation
Governance of digital transformation

Steering the ship through stormy waters

New technologies have a significant potential to augment, disrupt or replace existing business models. The risks brought by new technologies are likely to have a broad impact across the enterprise and therefore it is pivotal that businesses reflect on whether their existing governance models are fit for the future and able to navigate the considerable existing and upcoming volume of change. This includes having a firmer grasp of what the key new risk areas are, who owns these and how are they to be managed, monitored and mitigated.

How well defined is the concept of digital risk and who is being tasked with owning it?

With unprecedented levels of transformation occurring in many industries, it is not surprising that our survey results confirmed that digital risk is not yet well defined in many organisations. The majority are treating digital as an additional inherent risk driver for existing risk domains such as Information Security, Cyber, Data Privacy and Transformation. Interestingly, some respondents stated digital risk was well defined, but as a strategic execution risk (i.e. the role played by technology and data in enabling strategic objectives being reported at Board level), with the more granular operational risks remaining undefined. Another common theme was that those in the first line of defence tend to see digital risk as either a strategy or marketing risk or the stability of their digital channels (e.g. the mobile application), whereas Internal Audit tends to take a broader view and see it as cloud transformation, big data, and the adoption of emerging technologies such as artificial intelligence.

Most organisations appear to be focused on topical areas such as cyber and regulatory non-compliance, which would suggest that they have not yet explored the end-to-end risk implications of digital transformation, which has broader implications for risk management than cyber, data and regulation.

Some respondents highlighted a lack of digital expertise in control functions as a contributory factor to the absence of greater focus, with organisations often relying on ‘gut feel’ of the individuals tasked with owning it, as opposed to a structured governance approach as is the case with better understood domains such as cyber.

The impact on risk ownership

Clearly the challenge of gaining agreement on what constitutes digital risk feeds through to the clarity of, or lack of, ownership seen in many organisations. Our survey would suggest that, in most organisations, it resides either in IT, strategy or marketing functions, or is not well defined.

33% of survey participants noted digital risk being owned by the Chief Information Officer (CIO) (this was the most popular response across all regions). 14% gave their own category such as the CEO of the Digital function or ownership being dependent on the scenario (e.g. an issue with the mobile application versus a poor customer outcome from a digital channel). 12% suggested that ownership is not clearly defined and the remaining obvious players such as Chief Technology Officer, Chief Executive Officer and Chief Risk Officer all sat around the 8% mark.

Given the broad impact of digital across many areas of the business, including change, suppliers, finance, real estate, strategy and organisation design and culture, it is advisable to have a clear view of where the responsibility for managing digital risk lies.

The financial services and consumer products industries were the only two industry sectors to mention the emerging role of Chief Digital Risk officer.
Are current governance models aligned to the level of adoption, and are they scalable?

Figure 7. Comparing survey responses on the adequacy of governance approaches at different stages of adoption cycle with confidence levels around feasibility of scaling governance approaches in line with wider adoption

To what extent do you agree with this statement: “Our governance approach is right sized for our current level of adoption”

<table>
<thead>
<tr>
<th>Technology</th>
<th>Agree</th>
<th>Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet of Things</td>
<td></td>
<td>47%</td>
</tr>
<tr>
<td>Application programming interfaces</td>
<td></td>
<td>26%</td>
</tr>
<tr>
<td>Agile development</td>
<td></td>
<td>33%</td>
</tr>
</tbody>
</table>

How confident are you that your current governance approach around the following disruptive technologies will allow you to scale adoption effectively?

<table>
<thead>
<tr>
<th>Technology</th>
<th>Confident</th>
<th>Not Confident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet of Things</td>
<td>20%</td>
<td></td>
</tr>
<tr>
<td>Application programming interfaces</td>
<td></td>
<td>33%</td>
</tr>
<tr>
<td>Agile development</td>
<td>25%</td>
<td></td>
</tr>
</tbody>
</table>

Opportunity for creating a digital advantage

The broad impact of digital transformation creates linkages and dependencies between risk owners across the business that can prevent or slow down risk remediation. Risk teams have a role to play to make sure that governance models put the right people in the room, with the right information, and are underpinned by a culture of transparency and collaboration.
What areas of the organisation are involved in governing digital transformation?

Currently 73% of respondents have their technology function represented on the governance body tasked with managing digital transformation with the Accountable Exec, Operations, Strategy, Risk and CISO also frequently represented (in 37% of companies). Only 16% of organisations have HR represented on their digital transformation governance body with Supply, Manufacturing, Logistics and Procurement being represented in under 10% of organisations.

Respondents noted that the key functions driving digital transformation governance are technology, risk and accountable business units (74%, 40% and 39% respectively), which might suggest that risk functions have a seat at the digital transformation table but have not yet succeeded in turning strong governance into digital advantage. Half of respondents suggested that they have limited functional representation on the governance body tasked with managing digital transformation (three functions or less).

Have organisations defined what their appetite for risk is in the context of digital transformation?

Only 13% of organisations stated that they have clearly defined their risk appetite in relation to digital transformation. 46% of respondents have discussed risk appetite in the context of digital transformation but do not have anything formally defined or published, and 33% of organisations have not considered defining risk appetite specifically for digital transformation at all, although this was more common in organisations with under 1,000 people working on digital projects.

Are organisations using metrics to assess their risk exposure?

Approximately half (49%) of respondents said they are adopting the enterprise wide operational risk approach to defining risk metrics. Given the emerging risks highlighted in section 3 of this report, the question remains whether, in a digital environment, these traditional metrics provide sufficient coverage of the digital landscape. With only 7% of respondents saying they felt information provided to governance bodies is comprehensive and efficiently produced, there is clearly work to be done here.
Five opportunities to improve governance approaches highlighted by our survey respondents

Many survey participants offered their views on opportunities to enhance existing governance models. The overarching theme was the importance of aligning the governance model with that of the overall digital strategy, rather than operating in isolation. The top five recurring themes identified were:

**Educate business stakeholders not directly impacted by technology** – there is a perception that business teams do not always have visibility of the potential impact of changes to the technology estate, be it data or technical aspects, on the customer experience and brand reputation. Increasing their understanding will only add to an organisation’s ability to identify and manage risk.

**Remove organisational silos** – it was suggested that a joint effort between the business, technology and risk teams is required in order to avoid a one dimensional governance model and avoid a scenario where individual teams proceed, thinking it’s someone else’s responsibility to define the governance model.

**Define a technology adoption and implementation framework** – respondents stated that providing a consistent framework and structure allows for consistent reporting, and also sets out the agreed methodology to scale governance efforts in line with adoption from proof of concept to scale. Having a consistent framework in place may also avoid accountability for risk management being project based, rather than programme based, which may create variances in approaches across a portfolio.

**Identify and navigate competing organisational priorities** – whether it be increased speed to market at the same time as cutting costs, or extending the life of out of support infrastructure at the same time as investing in new modern architecture, there are likely to be conflicting priorities across the organisation that need to be identified and governed.

**Clarify the role of Internal Audit** – the role of Internal Audit in providing assurance over Digital Transformation appears unclear from our survey results, with only 15% saying their internal audit function has a strong impact and influence. Given the skillsets that sit within this function, this represents a missed opportunity for organisations to apply a degree of rigour and structure to their transformation efforts.
Areas of emerging risk as a result of digital transformation
Areas of emerging risk as a result of digital transformation

Paying sufficient attention to new risks, whilst still dealing with increased complexity of known risks

There is little doubt that the risk landscape continues to change rapidly and organisations find themselves attempting to manage known risks, such as cyber and data privacy, at the same time as trying to understand and address areas of emerging risk. As the line between business and technology teams continues to blur, emerging areas of risk are likely to have a greater strategic impact than traditional technology risks have done in the past.

What is seen as the primary source of emerging risk?

The overarching theme emerging from survey respondents is the integration of business and technology having an ever increasing impact across all risk categories within a traditional risk management framework, not just operational risk. With many existing risk frameworks having been based on principal risk categories defined before the levels of technology adoption we see today, assessing the impact of digital transformation exclusively against this lens is unlikely to be sufficient.

With the focus on cyber security and data privacy in recent years it is no surprise that organisations believe the top three areas of emerging risk are cyber (21%), data privacy (17%) and regulatory non compliance (12%). These top three responses were consistent across all lines of defence. However, some respondents gave the view those areas are no longer ‘emerging’ – awareness of these areas is high and in many cases a significant amount of work has gone in to reducing risk in these areas.

Digital transformation does add further complexity to these known areas though – an increase in digital assets and 3rd party integrations create additional cyber threat entry points, the use of vast volumes of data created by digital assets poses privacy and ethical considerations, and assurances on regulatory compliance can be difficult to obtain in the absence of prescriptive regulatory guidance.

Differences in opinion across the lines of defence emerge when looking beyond the top three answers. First line respondents cite ‘pace of change’ as the fourth area of emerging risk, second line respondents cite ‘third party relationships’ and third line respondents cite ‘adequacy of risk management process for digital’ (see Figure 8). This appears logical – with operational teams likely to be concerned about the speed at which they are being asked to deliver, risk teams likely to be more worried about the implications of the extended enterprise, and audit teams being concerned about whether the organisation is scaling their risk management capacity in line with the growth of the digital organisation. These are all valid concerns and heighten the need for effective governance and collaboration across the lines of defence to ensure risk remediation activities are prioritised in line with the needs of organisation rather than a particular function.

Is sufficient attention being given to understanding the implications of emerging risks?

Figure 8. After cyber, regulatory non compliance and data privacy the categories that respondents feel present the highest source of risk to the organisation varies by line of defence.

1st line
Pace of change

2nd line
3rd party relationships

3rd line
Adequate risk management process for digital
The increased complexity of the risk landscape

Other insights from our survey included examples of where the complexity of known risks is increasing (see Figure 9), where new technical knowledge is required to understand what needs to be done differently from a control perspective in relation to new technologies (e.g. logical access controls for a cloud implementation), and specific risks that, whilst it may be possible to categorise them under an existing operational risk category, may not have been covered in depth before. Examples of these include:

- **The impact of digital channels on fraud exposure for different customer segments** – i.e. is a bank customer more susceptible to fraud if they engage exclusively via specific channels such as web or mobile, as opposed to physical channels such as a branch?

- **Scaling risk** – one particular challenge revealed in the survey was in relation to dependencies on teams that sit outside of the digital function, and whether those teams are able to scale quickly enough as the volume of processes, customer journeys and change portfolio owned by the digital function grows over time.

- **Tooling risk** – as the digital estate grows, so does the plethora of tools required to support it. Many of these tools may not have historically been on the radar of control teams and therefore careful consideration should be given to the level of control required over tools such as automation consoles used for code deployments.

- **Change latency risk** – comments showed many digital teams would like to be able to release changes to production more often but are unable to do so because of constraints elsewhere in the organisation. Aside from the cost and strategic risk of not being able to deliver change quick enough, longer lag times between being ready to deploy and being able to deploy often mean higher number of changes being rolled in to each release, making it harder to identify the cause of a problem if incidents occur.

- **Culture and organisational design risk** – as organisational structures to enable digital transformation evolve, with varying degrees of autonomy, different reporting lines and governance structures, the impact of a suboptimal organisation design could play a major role in an organisation’s ability to deliver.

Opportunity for creating a digital advantage

Helping the organisation to understand and proactively manage the interdependencies between risk classes in a digital environment, such as the linkages between conduct risk, third party risk and operational risk, will contribute to strengthening operational resilience. Using data and automation to do this quickly provides an even greater advantage.
Does a digital organisation require a rethink of the traditional risk framework?

Logical access to system and data

Roles within delivery teams are increasingly fluid, suggesting the blurring of lines between traditional roles in design, development, testing, environment management, release management and application support. This poses the question as to whether 'role based' approaches to restricting access are still effective when individuals are required to adopt more than one role.

Change management

As the complexity of the digital estate increases and the need for change to be delivered at speed increases, a one size fits all approach to governing change can create bottlenecks.

Incident management

As processes that traditionally span different teams become automated, such as code deployments and release management, who takes the lead in the event of an incident?

Data governance

Digital channels provide an enormous amount of data about customer behaviour, creating a significant reliance on data quality for commercial success. Remaining regulatory and ethically compliant becomes increasing complex.
**Global Perspectives – Do respondents feel operational resilience is enhanced or reduced overall as a result of digital transformation?**

<table>
<thead>
<tr>
<th>Reduced</th>
<th>No Impact</th>
<th>Enhanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>24%</td>
<td>21%</td>
<td>55%</td>
</tr>
</tbody>
</table>

**Businesses in the Americas are more likely to see digital transformation as reducing operational resilience**

<table>
<thead>
<tr>
<th>Reduced</th>
<th>No Impact</th>
<th>Enhanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>21%</td>
<td>17%</td>
<td>62%</td>
</tr>
</tbody>
</table>

**Those in Risk and Audit roles appear to have a more positive outlook on the impact of digital transformation on operational resilience**

<table>
<thead>
<tr>
<th>Reduced</th>
<th>No Impact</th>
<th>Enhanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>26%</td>
<td>22%</td>
<td>52%</td>
</tr>
</tbody>
</table>

**Technology businesses are more convinced that digital transformation is enhancing operational resilience**

<table>
<thead>
<tr>
<th>Reduced</th>
<th>No Impact</th>
<th>Enhanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>40%</td>
<td>11%</td>
<td>49%</td>
</tr>
</tbody>
</table>
How is the risk landscape expected to change over the next three years, and what challenges is this presenting?

Many survey respondents believe the risk landscape is changing quickly, and the extent to which this results in increased or decreased risk exposure for organisations depends on their ability to adapt and respond.

Some key challenges highlighted by respondents include:

• **Maintaining control as third party integration increases** – organisations reported increasing efforts to incorporate third parties into their value chains – whether that be with established technology vendors or technology start ups. Our results suggest that Sales and Marketing, Strategy and Technology departments are leading the way in forming these relationships, with a broad range of opinions on how well integration efforts have gone so far ranging from ‘easy’ to ‘impossible’. Challenges stated were centred on achieving the right level of governance, both initially and at scale, around topics such as security, business continuity and data, especially when risk teams are not involved up front, and in some cases after contracts have already been signed. Examples given of techniques to overcome these challenges included treating the third party as a partner rather than a vendor, larger organisations providing start ups with access to skills and resources to get them up to the required level, and conducting proof of concepts with upfront involvement from risk teams to ensure that risk is not overlooked from day one.

• **Understanding concentration risk** – whether it be moving infrastructure to a single cloud provider, outsourcing a critical part of the customer journey, such as onboarding, to a single third party, or automation of core processes, concentration risk, a critical dependency on a single process or provider, was perceived to be on the rise. The challenge highlighted in our survey is one of ownership – whose job is it to understand concentration risk and monitor it on behalf of the organisation.

• **Adapting the operating model as change becomes business as usual** – continual, incremental change is a core part of product development. With the volume and frequency of change having increased dramatically, change is effectively already a BAU process for certain change categories, but not all. This is driving process change (such as the increased use of automation), cultural divergence (between digital and non digital teams) and organisational structure changes (such as the desire for increased autonomy for delivery teams tasked with delivering change quickly).

• **Providing adequate oversight of automation** – the extent to which organisations leverage automation, whether it be through deployment of robotic process automation software, automating data flows between systems in an end to end customer journey, or automatically provisioning environments and running automated test scripts, is likely to increase. As it does, one of the key questions to answer will be one of accountability for automated processes spanning multiple departments, including those partially automated processes that are then handed off to manual processes elsewhere in the organisation.

• **Closing the technical knowledge gap outside of technical teams** – some organisations noted concerns around the speed of change across the digital estate outstripping the speed at which an organisation can understand and manage the associated risks. This is particularly pertinent for traditional technology risk and audit teams, who are tasked with trying to keep up with technology trends when technical roles are not their full time job.
The operating model for risk
Enabling control in times of change and ambiguity

The structure of the organisation is slowly changing – digital transformation is driving new business models, new technology implementations, new processes and ways of working, and evolving organisational structures. This constant flux creates a challenging environment to establish ownership and accountability for risk, as well as responsibility for execution of core risk management processes and applicability of those processes to different parts of the organisation. The traditional functional model for risk management must adapt accordingly.

How is the adoption of disruptive technology changing what’s required from risk management at an operational level?

Our survey shows that risk management activities are undoubtedly evolving as the business adapts to a digital economy. The most commonly recognised impacts across all respondents were:

- the increased importance of continuous monitoring versus retrospective assurance (47%)
- the need for more technical skills (46%)
- a need to redefine the engagement model for risk and control (46%)
- the need to tailor the risk management approach for each disruptive technology (42%)

Whilst these top four categories were broadly consistent across respondents, there were some variances across different reporting lines.

Those in the second and third lines of defence identified redefining the engagement model as the main priority, suggesting that these teams recognise the need to evolve the way they interact with operational teams to remain effective. Those in non risk roles in the first line put the increased importance of continuous monitoring first. This may have been anticipated given first line stakeholders are likely to value insight from risk teams that drives day to day escalations and decision making, rather than retrospective point in time interventions.

Interestingly, first line respondents in risk roles put the need for more technical skills as their main priority, as well as including the need for ‘increased speed’ in their top four. This is understandable given they are likely to be managing day to day technical issues.

Many of the changes in the role of the risk management function highlighted relate to the increased criticality of risk management on the front line, and the increased demand for a risk capability amongst operational and change teams. These changes were neatly summed up by one respondent as more of an “enabling role” rather than just the “protect” role traditionally played by the Risk function itself.

Dialling up risk engineering and analytics on the front line

Figure 14. The expanding role of a Risk Manager on the front line
How are the roles and responsibilities of the risk management function evolving?

Survey respondents were quick to highlight that the overarching objectives of traditional risk management activities remain as relevant as ever, but execution methods are changing to better align outputs to senior management needs – proactive, preventative and predictive rather than reactive, retrospective and detective. This means risk management activities are evolving, with examples highlighted by the survey including:

• **A greater involvement in solution design** – there are clear signs of an expanding remit for risk teams that includes the ‘factory’ – the digital delivery teams tasked within delivering the products and solutions that underpin many of the changes driven by digital transformation. Incorporating a risk and control lens in to solution design from day one represents a big opportunity for organisations to reduce assurance costs further down line.

• **Increased emphasis on data analysis** – a common trend identified was that management now expects predictive analysis rather than detective results, and hence the increased reliance on analysis of data generated within a digital environment.

• **Increased scope of risk coverage** – respondents called out the fact that digital transformation is increasingly touching many different parts of the organisation, broadening the potential number of risks that risk teams are required to understand and advise on. This suggests a need for risk leaders who understand the broader digital organisation.

• **Embedding controls within process automation initiatives** – as organisations expand their use of automation, leading organisations are actively seeking out opportunities to embed controls within newly automated processes, changing the nature of future assurance models from manual and periodic to automated and continuous.

• **Moving away from the ‘annual’ waterfall style assurance cycle** – many traditional programmes of assurance follow an annual cycle, with defined planning, testing, reporting and remediation cycles that repeat year on year in order to allow management to attest to the effective operation of controls. Organisations are exploring how they can move towards a continuous, agile assurance approach that puts a ‘screen on the wall’ which can be used to inform decision making, rather than a bi-annual assurance report.

**Opportunity for creating a digital advantage**

There is huge potential to reduce the cost of assurance by designing automated controls that, if done right, would allow assurance teams to focus on the design of the automated control rather than the costly, manual, sample based exercise of operating effectiveness testing.
What impact is the variance in adoption of agile ways of working having on the organisation?

Our survey results suggest that very few risk management functions have been able to successfully adopt an agile culture – only 9% of respondents said this was the case. This contrasts to what we see in digital delivery teams where an agile culture has become the default way of working. This divergence in adoption goes some way to explaining why over half of respondents (55%) said that their organisation had been unsuccessful, or only had limited amounts of success, in adapting risk management techniques for agile delivery. In some cases, some respondents stated their risk teams were “not even on the pitch” when it came to assessing the risks of agile delivery. Our own observations reflect frustrations on both sides of the fence – digital delivery teams wanting to deliver faster, recognising that strategically, the cost of delay for the organisation is high, whilst risk teams are concerned at the impact of going faster without clear articulation of how the right level of control is being maintained.

Only 9% of respondents said their risk management function had successfully adopted an agile culture.

When asked how successful their organisation has been at adapting risk management techniques for agile delivery, 55% of respondents said ‘not at all’ or ‘we’ve tried but with limited success’.

Opportunity for creating a digital advantage

Given the amount of investment being spent on developing new digital products and solutions, this represents a call to action for risk teams to define their engagement model with digital delivery teams, and demonstrate the value they can provide by helping to reduce the time and cost of change for the organisation.

What could agile assurance look like?

Figure 15. The principles behind an agile assurance model

Continuous delivery
Realise business outcomes

Risk taxonomy
Identify taxonomy of inherent risks

Prioritisation
Prioritise delivery based on business value

Digital delivery

Agile assurance

Business outcomes
Identify business outcomes

Continuous assurance
Control design, implementation and assurance

Prioritisation
Refine risk backlog based on risk reduction value to the business

Beyond the hype | Global Digital Risk Survey 2019
What could the future operating model for managing risk look like?

Attempting to manage today's risk environment with an operating model designed for a pre-digital world is unlikely to be optimal. We believe a true multi-disciplinary model may be required for organisations wishing to derive greater value from their risk management capability – potential examples of the make-up of a future risk management capability include:

**Centralised capabilities**

- **Technology Intelligence** – experienced technical experts who understand the risks associated with different types of technology, as well as the enterprise architecture, and can oversee the integrity and completeness of the risk taxonomy.

- **Digital Risk Solutions Factory** – software engineers who can design, build, test and deploy solutions, whether it be to enable risk management activities with technology or build the risk and control framework into the existing technology stack to enable continuous monitoring.

- **Risk Operations** – risk and control experts who can design and run core risk management processes, feed in requirements to the solutions factory and provide a 'service desk' function to aid operational staff managing risk day to day.

- **Risk Analytics** – data scientists experienced in analysing large data sets to proactively identify risk insights by combining different data sets together (e.g., fraudulent transactions in relation to different digital channels).

- **Risk Experience** – service design experts and product managers who engage with internal stakeholders to develop and evolve risk offerings provided, removing friction and increasing satisfaction and engagement with risk processes across the organisation. See Figure 16.

- **Risk and control assurance** – a centralised assurance capability that can perform independent assurance on behalf of other teams, independent of where they sit in the organisation.

**Decentralised capabilities**

- **Product/Service/Channel Risk Owners** – experienced digital risk experts responsible for managing both the technical and commercial aspects of risk associated with a particular product, service or digital channel.

- **Risk Squads** – cross-functional teams formed from a variety of different disciplines tasked with delivering specific objectives in short sprints i.e. control design sprints, control implementation sprints or risk remediation sprints.

**Digitally enabling manual tasks**

**A case study on an automated solution to assess quality and coverage of a control library**

One client was looking to review the quality of over 8,000 control instances documented in their control library, with the estimated manual effort required put at 26 weeks. 8,000 controls were uploaded and analysed by Deloitte's automated control library assessment tool, Controls Intelligence, in 45 minutes.

Root cause analysis delivered a remediation roadmap and provided insight into remediation priorities. Specific teams were found to be sub-standard in control creation, thereby allowing training in those specific teams to be delivered.
How can risk teams free up capacity to make the transition whilst still keeping the lights on?

In many industries there will always be a focus on cost, making it more difficult to secure funding for change initiatives over and above what’s required to keep the lights on. The question therefore becomes how can organisations free up capacity within existing teams to make small, incremental steps towards the end goal. We see three primary focus areas that could be explored:

Many every day risk management activities remain manual, but could be technology enabled – manual manipulation of data for risk reporting, chasing for status updates for risk packs, assessing the coverage of the existing control library, performing quality assurance over control assessments performed by countries around the world. Many of these activities could be improved by enabling them with low cost technology solutions (see case study on previous page).

Build engagement with existing technical experts already in the organisation – many organisations will have a growing number of technical experts in the organisation who have an interest in demonstrating effective control in order to drive further adoption of more technologies. The risk function could proactively identify and build relationships with these individuals.

Be relentless in eliminating non value adding tasks – in any process with multiple steps there are likely to be opportunities to streamline. Revisiting existing processes with a ‘lean’ mindset is likely to identify opportunities to redirect valuable resources to more value generating activities.

Improving RX

Figure 16. A better risk experience within the organisation, powered by technology

The Risk Experience

Simple
A frictionless engagement model that drives engagement and adoption of a risk aware culture

Tech enabled
Supported by intelligent technology solutions that drive consistently high ratings from users

Challenging, but collaborative
Fact based, collaborative processes that drive the right results for the organisation

Transparent
Rationale that is visible and understood by all

Drives decision making
Quick informed decision making that creates value
Use of disruptive technology to manage risk digitally
Use of disruptive technology to manage risk digitally

A largely untapped opportunity

Managing risk at scale is a complex task. Whilst some industries have been more successful than others at using technology to manage risk, many organisations still manage key assets and processes such as risk taxonomies, control libraries and risk assessments in standalone, legacy systems, or spreadsheets. Significant opportunities to apply newer modern technology to drive better value from risk management spend are emerging, but in order for those initiatives to be successful the right foundations must be in place – a consistently understood risk taxonomy and control library, robust and mature processes, and most importantly, clear ownership and responsibility for risk.

How effective is risk management tooling today?

Our survey indicated that overall 60% of respondents rate the effectiveness of current risk management tooling as five, or less, out of ten (77% Americas, 56% EMEA, 59% APAC). This is a worrying indicator of organisations’ inability to deal with the increased speed of change, complexity and volume of activity that digital transformation is driving.

When asked what barriers exist that prevent organisations from improving the effectiveness of risk management tooling, some key themes emerged:

- Lack of knowledge of what’s now possible, and a lack of time to think about it
- Inability to integrate tools with legacy systems and across software packages
- Lack of alignment between operational tools and the risk management framework and processes
- Poor quality data
- The velocity of change which makes it difficult to gain agreement on approach and tools across different teams and functions
- Differences in the structure of control frameworks used across the organisation making it difficult to aggregate data across teams and functions
- Difficulty in articulating the business case for investment in tooling
- Cultural resistance to change.

Notably very few, if any, of the barriers above relate to a lack of technology capability. The barriers stated imply that the underlying reason for a lack of effectiveness of tooling has more to do with issues in the underlying risk management frameworks, processes, accountability models, technical knowledge of decision makers and culture. This suggests that if organisations can resolve these aspects first, then the technology exists to take big strides forward in their risk management capability.

Tech tooling
Figure 17. Categories of toolsets being used by organisations who adopted disruptive tech
How many organisations use disruptive technology to manage risk?

The survey highlighted that approximately one fifth of organisations are leveraging disruptive technology for core stages of the risk management lifecycle – risk identification (19%), risk monitoring (21%) and risk reporting (17%). We expect those numbers to grow as organisations currently piloting approaches (35%) build out use cases to widen adoption.

When asked about the specific use cases where modern technologies were being deployed, the examples given related primarily to the use of advanced analytical capability in domains such as anti money laundering, fraud and cyber. With typically large operational data sets these are a logical place to start given technology now allows for analysis of entire data sets where historically a sample based approach has been taken.

There is also a fairly well understood business benefit in these areas, such as a tangible percentage reduction in fraudulent payments, which helps to justify upfront investment in these technologies. The survey results show that the majority of organisations are heavily relying on mature vendor software packages (70%), which is as expected given the use cases outlined above (see Figure 17).

A number of emerging use cases for typically manual risk management processes were also highlighted by the survey – see Figure 18. With only 9% of respondents applying new technology for assurance activities such as controls testing that typically involve a large degree of manual effort, there are potentially opportunities for further efficiency gains.
The impact of the current state of risk management tooling

There are no silver bullets – finding and integrating the right combination of tools to support management of risk has proved itself to be extremely difficult, and to a certain extent, it appears to be getting harder as digital transformation drives cultural, process, structural and technology changes. Business and technology teams, risk managers and enterprise risk teams all play a role in managing risk, but often they are faced with different demands, pressures and requirements that makes alignment of tooling strategy increasingly difficult.

Whilst it is fairly straightforward to identify a technology solution for a specific use case, such as fraud analytics, when it comes to supporting manual risk management processes that span more than one team or department and require a consistent aggregation framework to report up the hierarchy, as risk management processes do, we see a lot of organisations struggling. Many have defaulted to using existing tooling and supplementing it with manual consolidation, analysis and reporting that brings disparate data sources together. This might explain the low effectiveness ratings shown by our survey, especially as it comes at a time when expectations have risen considerably as a result of the incredibly effective and user friendly technology that has become part of everyday life. This also goes some way to explaining the low scores given by survey respondents to the adequacy of information being provided to governance forums, given the manual nature of how this data is being pulled together.

The primary impact of this current landscape is that it may become more difficult for management to see the wood from the trees, impacting their ability to focus on what’s most important and make the right decisions to reduce risk. In many cases the most common areas of risk exposure – regulation, cyber security as examples – are actively monitored, but other less obvious or immediate risk categories may not be adequately managed and may destroy value for the organisation.

Turning the conversation on its head – what is actually required for an effective risk management system, and how could technology be used to facilitate that?

The potential value creation from the application of disruptive technology to specific risk management use cases is becoming clearer, but many organisations might want to revisit the foundations of a robust risk management culture first before diving in to large scale investment in new solutions. Some key questions to be considered include:

- does the culture at all levels reflect a true understanding of the value to the organisation of managing risk well, and is what’s required from individuals at all levels clear?
- is the taxonomy of inherent risks consistently understood across the organisation, and aligned to control libraries that reflect what happens on the ground?
- are enterprise wide risk management processes mature and stable, and do front line teams understand how they apply to what they do every day?
- are processes in place to triage data and enforce data quality, as opposed to just capturing and reporting data?
- are the right decision making processes and escalation routes well defined and aligned to the formal governance committees?
What new possibilities are opening up as more modern technology solutions become mainstream?

We observed a number of growing opportunities to leverage modern technology to redefine how tooling supports the risk management agenda:

- **Leveraging investments in process automation to embed control by design** – with many organisations embarking on automation programmes, whether that be through robotic process automation, or automating core IT processes such as release management, building control requirements in from the start of the process will reduce the need for, and associated costs of, manual forms of assurance down the line.

- **Embedding a control lens in day to day operational tools** – building control effectiveness views, aligned to the organisational risk framework, into operational tools used on a day-to-day basis (e.g. to maintain customer facing services or monitor availability of digital channels) is likely to enable management to demonstrate, in a language that is understood by those in more formal risk management roles, how risk is being managed.

- **Generate new insights by integrating data from different systems** – live services are often delivered through the combination of different processes from across many different teams. Organisational silos often prevent the effective sharing of knowledge and data that, when combined with knowledge and data from another team, could create a valuable source of insight. Combining incident data with control library data to understand what went wrong is an example of this.

- **Tech enable the manual risk management lifecycle** – there will always be an element of risk management activity that needs to be done manually – from identification through assessment to remediation and reporting. Enabling these manual processes with technology rather than spreadsheets provides an opportunity to improve data quality through effective triage, track and monitor remedial actions, enforce sequential consistent workflows for visibility of decision making and automate reporting.

- **Improve the user experience** – many organisations aspire to improving their risk management culture and a better understanding of the value of robust risk management. Put simply, in order to drive change in these two areas and engage the workforce, the tools used need to do simple things well. People must want to use the tools available to them because it makes their life easier, not harder.

- **Drive collaboration** – the use of collaboration tools and techniques such as wireframing, where the type of content and most appropriate layout (e.g. for a webpage) are defined based on user needs, are fundamental to designing digital propositions. A similar approach and concept could be used within the risk environment to improve the format and layout of key risk reports, which in turn would allow committees, often driven by the structure of the data in front of them, to focus on the right things.

---

**Opportunity for creating a digital advantage**

Automating the administrative aspects of managing risk represents a significant opportunity for organisations to improve data quality, make faster decisions and free up capacity to think more strategically rather than just keep the lights on.
Is the biggest digital risk, people risk?

For all the debate around the future impact of disruptive technology on the workforce, an organisation’s ability to get the best out of its human capital will always be a key driver in determining its success. Individuals are at the heart of what organisations do, and whilst having the right person in the right role has always been crucial, having the right people managing risk is now more important than ever.

Is it time to revisit the traditional role of a technology risk manager in an increasingly complex and integrated corporate environment?

Continued technological advancement, the ever increasing pace of change, and the resulting challenges in agreeing and aligning priorities across the different layers of an organisation makes managing technology risk an increasingly complex task. It is therefore unsurprising that we see a lack of conviction from leadership that their current teams have the appropriate skillset to manage risk in a digital organisation – a term we refer to as the confidence gap, with only 19% feeling ‘fully confident’ their teams are equipped with the skillset to do the job (see Figure 19 below).

The responses to our survey imply that the risk manager role is becoming focused towards influencing, coordinating, collaborating and communicating with others in the organisation, often outside the Risk function itself, to get the job done, rather than assuming the responsibility of managing the risk itself as the job title ‘Risk Manager’ implies.

The cause of the confidence gap – the emergence of the Digital Risk Manager

Figure 19. The increasing integration of business and technology teams in digital delivery teams is creating the need for digital risks managers

<table>
<thead>
<tr>
<th>The Digital Risk Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisations are seeking individuals who understand all aspects of the digital product lifecycle and drive an integrated, product view of risk understood by business and technology leadership</td>
</tr>
</tbody>
</table>
How are the skills required from a risk manager changing?

Our survey showed the skills deemed most important when recruiting new candidates into technology risk roles are a combination of technical and business experience (72%) and prior risk management experience (66%). More interestingly, the data shows the increasing importance being placed on recruiting candidates with specific technical experience (49%) and a problem solving ‘agile’ mindset (46%). We have called this the ‘Butterfly’ effect, as the traditional risk manager skillset broadens out to place greater emphasis on a blend of technical and commercial skills, as well as the ability to adapt and thrive in both an agile and traditional corporate environment (see Figure 20 below).

The ‘Butterfly’ effect

Figure 20. How the current operating environment is changing the skills required from risk professionals

The need for risk managers with deep technical expertise is also on the rise, to help organisations understand how traditional control frameworks apply to disruptive technologies.

Opportunity for creating a digital advantage

- **Be clear on what you need** – being clear on the skillsets and behaviours you are looking for allows you to look for candidates in the right places. Consider looking to the left and right of traditional recruitment channels.

- **Be flexible with the prerequisites for the job** – being prescriptive on the risk management experience candidates must have to apply might deter the type of candidates with the skillsets you’re looking for.

- **Understand what your ideal candidate is looking for** – this understanding will allow you to create the environment where candidates find you, rather than you finding them.
The impact of not addressing the widening skills gap

Our survey suggests the gap between the skillset required to navigate the evolving risk landscape and the skillset of the traditional technology risk manager has been widening for a number of years. Organisations who are unable to close the gap are likely to find it increasingly difficult to manage risk effectively. As digital transformation continues to disrupt many industries, we see five key implications for those with a risk management capability lacking in the core skillsets now required:

- **Slowed adoption of new technology and slow delivery of change** – our survey highlighted a lack of talent as one of the primary barriers to scaling the adoption of disruptive technology, as well as a key barrier in reducing the time taken to convert ideas into live solutions. This highlights the importance of having a talent strategy that aligns to the needs of the business.

- **Risk blind spots across the organisation** – pockets of risk exposure that go unmanaged, either because of a lack of the knowledge and experience required to identify, understand and manage the risk, or because those that have the relevant experience and knowledge do not see it as their responsibility to manage that risk.

- **A lack of engagement with risk management activities at grass roots level across the organisation** – the most successful and robust organisations are able to successfully align front line teams managing risk on a daily basis with enterprise wide operational risk processes. The skills and influence of those in formal risk management roles play a crucial role in facilitating this.

- **Reallocation of risk management funding away from Risk function itself** – risk management functions that are unable to demonstrate the value they provide will likely see their funding cut, as other functions in the organisation pick up the mantle for defining more effective assurance processes.

- **Inability to retain high performers** – top talent is in high demand as the first wave of ‘digital natives’ reach senior management positions and the onus is on organisations to make permanent risk management roles attractive in order to retain high performers. With attractive offers on the table from industry leaders, many high performers will not be prepared to wait for their own organisations to ‘catch up’.

Talent tactics – what can be done in the short term to make the most of existing talent pools?

- **Harness people’s natural curiosity for learning, but provide a framework aligned to the needs of the business** – the need to stay up to date has never been more pressing, but a situation where everyone is expected to know everything can be counterproductive.

- **Embed a risk aware culture via the on-boarding process** – as organisations hire staff from outside of their own industry sector, this can create an awareness gap if individuals are moving from a non-regulated industry to a regulated one.

- **Train risk management staff to apply the ‘digital’ skillset in their own day to day activities** – the emergence of the ‘digital’ skillset, the ability to research user behaviours, define problem statements, create solutions, conduct usability testing, are all skills that could be deployed in updating methods for managing risk and providing assurance.

- **Understand the different sources of talent available to you** – the skillset now required to manage risk effectively is so broad that it is unlikely to be found in one individual, despite the ‘risk manager’ job title still prevailing. This makes it increasingly important to have access to a broad range of skillsets and be able to ramp up and ramp down resource quickly.

- **The emergence of Risk Mentors in addition to Risk Managers** – given the scale and complexity of change in many industries, answers to our survey revealed the emergence of the ‘risk mentor’ role i.e. experienced individuals within the organisation who have relevant prior experience offering advice to peers on pitfalls and strategies to manage risk.
Long term strategy – delivering the vision for risk management across the organisation, not just for the Risk function

With the pace of change over the last 15 years there have been some significant issues to address as organisations try to embed a sustainable operating model to embed the right risk management culture and behaviours within technology teams over the long term. Getting risk management teams across different lines of defence working well together, at the same time as maintaining an appropriate level of independence, has proved challenging for many organisations.

Many organisations aspire to having a risk management capability that not only protects the organisation but also drives performance and adds value to the bottom line. In order to do that many organisations have a vision for risk management that involves culture change as well as leveraging new capabilities such as advanced analytics, automation and artificial intelligence to provide real time insight that drives decision making.

Whether the method of achieving this vision involves a build, partner or buy approach, an organisation’s success is likely to be dependent on having the right talent strategy in place. Simply hiring the best talent, on its own, is not likely to be enough. Those in leadership roles tasked with delivering on the vision need to be comfortable dealing with ambiguity in the short term and excel at influencing and collaborating with others across the organisation so that they can provide the platform for their teams to deliver the vision.

What are others doing around the world?

Figure 21. Examples of talent initiatives given by survey respondents

Canada
- Formal training on LEAN principles and the emergence of a ‘Risk Squad’ concept

United Kingdom
- Reverse mentoring where less digitally savvy executives are mentored on technology by junior, digitally savvy employees

Norway
- Risk and Technology teams attending courses and conferences together to develop common understanding of risk

Japan
- Sharing of knowledge with other organisations to combine areas of expertise

Ireland
- Formally defined digital learning pathway to encourage a consistent baseline of knowledge for all staff

Luxembourg
- Regular workshops with other departments to encourage collaboration, knowledge sharing and transparency

Italy
- A focus on employee led learning through the adoption of ‘learn to learn’ principles

Australia
- Rotational secondments of risk managers in to Technology roles and across the lines of defence

New Zealand
- Diversification – no employees whose sole specialisation is just risk management
What are the benefits of getting it right?

Over the last 10 years technology has fundamentally redefined how many of us live our lives. We are now at a point where many digital natives, those who have grown up with technology from an early age, are starting to reach senior management level in their careers. This represents a huge opportunity for organisations to define their long term plan to build a digital risk capability, attract digitally savvy talent and provide a career platform for top performers for the next 20 years. This window of opportunity to get ahead of the pack is unlikely to last forever.

As the operating environment gets increasingly complex, those organisations that are able to simplify their risk management approach so that it is widely understood and embedded in to day to day activities are likely to have a higher chance of successfully embedding a culture where operational teams ‘self identify’ and manage risks without relying on a dedicated risk manager to do it for them.

Opportunity for creating a digital advantage

To a certain extent, the biggest talent issue for organisations in relation to risk management, may sit outside the Risk function. Those in risk management roles are often outnumbered many to one when compared with the rest of the organisation. We therefore see an opportunity available to organisations to improve their risk position is to get people outside of traditional risk management teams and roles thinking through a risk and control lens.
Authors and Contributors

Authors

Rob Dighton
Director
Technology and Digital Risk
rdighton@deloitte.co.uk

Cherry Seaborn
Manager
Technology and Digital Risk
cseaborn@deloitte.co.uk

Dimitar Milanov
Senior Manager
Technology and Digital Risk
dmilanov@deloitte.co.uk

Contributors

Stephen Ley
Global Lead Partner
Technology and Digital Risk
sley@deloitte.co.uk

Tom Bigham
Partner
Technology and Digital Risk
tbigham@deloitte.co.uk

Charlotte Gribben
Partner
Technology and Digital Risk
cgribben@deloitte.co.uk
# Global contacts

<table>
<thead>
<tr>
<th>Americas</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Brazil</td>
<td>Rodrigo Mendes Duarte</td>
<td><a href="mailto:rodrigomendes@deloitte.com">rodrigomendes@deloitte.com</a></td>
</tr>
<tr>
<td>Canada</td>
<td>Nathan Spitse</td>
<td><a href="mailto:nspitse@deloitte.ca">nspitse@deloitte.ca</a></td>
</tr>
<tr>
<td>Caribbean and Bermuda Countries</td>
<td>Brette Henshilwood</td>
<td><a href="mailto:brett.henshilwood@deloitte.com">brett.henshilwood@deloitte.com</a></td>
</tr>
<tr>
<td>Chile</td>
<td>Oscar Bize</td>
<td><a href="mailto:obize@deloitte.com">obize@deloitte.com</a></td>
</tr>
<tr>
<td>LATCO</td>
<td>Jorge Hernandez</td>
<td><a href="mailto:jorgehernandez@deloitte.com">jorgehernandez@deloitte.com</a></td>
</tr>
<tr>
<td>Mexico</td>
<td>Doris Gomes</td>
<td><a href="mailto:dorgomes@deloittemx.com">dorgomes@deloittemx.com</a></td>
</tr>
<tr>
<td>USA</td>
<td>Daniel Soo</td>
<td>ds <a href="mailto:oo@deloitte.com">oo@deloitte.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Asia Pacific</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>Jonathan Goldman</td>
<td><a href="mailto:jonathangoldman@deloitte.com.au">jonathangoldman@deloitte.com.au</a></td>
</tr>
<tr>
<td>China</td>
<td>Tonny Xue</td>
<td><a href="mailto:tonxue@deloitte.com.cn">tonxue@deloitte.com.cn</a></td>
</tr>
<tr>
<td>India</td>
<td>Vishal Jain</td>
<td><a href="mailto:jainvishal@deloitte.com">jainvishal@deloitte.com</a></td>
</tr>
<tr>
<td>Japan</td>
<td>Shoichi Morimoto</td>
<td><a href="mailto:shmorimoto@deloitte.com">shmorimoto@deloitte.com</a></td>
</tr>
<tr>
<td>Japan</td>
<td>Yasuhide Onuma</td>
<td><a href="mailto:yasuhide.onuma@tohmatsu.co.jp">yasuhide.onuma@tohmatsu.co.jp</a></td>
</tr>
<tr>
<td>New Zealand</td>
<td>Reenesh Bhana</td>
<td><a href="mailto:rbhana@deloitte.co.nz">rbhana@deloitte.co.nz</a></td>
</tr>
<tr>
<td>Singapore</td>
<td>Philip Chong</td>
<td><a href="mailto:pchong@deloitte.com">pchong@deloitte.com</a></td>
</tr>
<tr>
<td>Singapore</td>
<td>Vineet Sinha</td>
<td><a href="mailto:vsinha@deloitte.com">vsinha@deloitte.com</a></td>
</tr>
<tr>
<td>Taiwan</td>
<td>Mike I. Chang</td>
<td><a href="mailto:mikeichang@deloitte.com.tw">mikeichang@deloitte.com.tw</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EMEA</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>Alexander Ruzicka</td>
<td><a href="mailto:aruzicka@deloitte.at">aruzicka@deloitte.at</a></td>
</tr>
<tr>
<td>Belgium</td>
<td>Johan Van Grieken</td>
<td><a href="mailto:jolangrieken@deloitte.com">jolangrieken@deloitte.com</a></td>
</tr>
<tr>
<td>Cyprus</td>
<td>Chrysovalantis Dikomitis</td>
<td><a href="mailto:cdikomitis@deloitte.com">cdikomitis@deloitte.com</a></td>
</tr>
<tr>
<td>Finland</td>
<td>Tuomo Salmi</td>
<td><a href="mailto:tuomo.salmi@deloitte.fi">tuomo.salmi@deloitte.fi</a></td>
</tr>
<tr>
<td>France</td>
<td>Gregory Abisror</td>
<td><a href="mailto:gabisror@deloitte.fr">gabisror@deloitte.fr</a></td>
</tr>
<tr>
<td>Germany</td>
<td>Alexander Huffer</td>
<td><a href="mailto:ahuffer@deloitte.de">ahuffer@deloitte.de</a></td>
</tr>
<tr>
<td>Ireland</td>
<td>Colm McDonnell</td>
<td><a href="mailto:cmcdonnell@deloitte.ie">cmcdonnell@deloitte.ie</a></td>
</tr>
<tr>
<td>Israel</td>
<td>Simeon Zimbalist</td>
<td><a href="mailto:szimbalist@deloitte.co.il">szimbalist@deloitte.co.il</a></td>
</tr>
<tr>
<td>Italy</td>
<td>Giuseppe Mazzotta</td>
<td><a href="mailto:gimazzotta@deloitte.it">gimazzotta@deloitte.it</a></td>
</tr>
<tr>
<td>Italy</td>
<td>Andrea Schiavon</td>
<td><a href="mailto:aschiavon@deloitte.it">aschiavon@deloitte.it</a></td>
</tr>
<tr>
<td>Luxembourg</td>
<td>Irina Gabriela Hedea</td>
<td><a href="mailto:ighedea@deloitte.lu">ighedea@deloitte.lu</a></td>
</tr>
<tr>
<td>Malta</td>
<td>Ivan Spiteri</td>
<td><a href="mailto:ispiteri@deloitte.com.mt">ispiteri@deloitte.com.mt</a></td>
</tr>
<tr>
<td>Middle East</td>
<td>Tariq Ajmal</td>
<td><a href="mailto:tajmal@deloitte.com">tajmal@deloitte.com</a></td>
</tr>
<tr>
<td>Netherlands</td>
<td>Marko van Zwan</td>
<td><a href="mailto:mvanzwam@deloitte.nl">mvanzwam@deloitte.nl</a></td>
</tr>
<tr>
<td>Norway</td>
<td>Erling Pettersen Hessvik</td>
<td><a href="mailto:ehessvik@deloitte.no">ehessvik@deloitte.no</a></td>
</tr>
<tr>
<td>Spain</td>
<td>Manel Carpio</td>
<td><a href="mailto:macarpio@deloitte.es">macarpio@deloitte.es</a></td>
</tr>
<tr>
<td>Switzerland</td>
<td>Michel Simantirakis-Aller</td>
<td><a href="mailto:msimantirakisaller@deloitte.ch">msimantirakisaller@deloitte.ch</a></td>
</tr>
<tr>
<td>Turkey</td>
<td>Cuneyt Kirlar</td>
<td>c <a href="mailto:kirlar@deloitte.com">kirlar@deloitte.com</a></td>
</tr>
<tr>
<td>UK</td>
<td>Charlotte Gribben</td>
<td>c <a href="mailto:gribben@deloitte.co.uk">gribben@deloitte.co.uk</a></td>
</tr>
<tr>
<td>UK</td>
<td>Tom Bigham</td>
<td><a href="mailto:tbigham@deloitte.co.uk">tbigham@deloitte.co.uk</a></td>
</tr>
<tr>
<td>Russia</td>
<td>Denis Lipov</td>
<td><a href="mailto:dlipov@deloitte.ru">dlipov@deloitte.ru</a></td>
</tr>
<tr>
<td>South Africa</td>
<td>Keshnee Naidoo</td>
<td><a href="mailto:kesnaidoo@deloitte.co.za">kesnaidoo@deloitte.co.za</a></td>
</tr>
</tbody>
</table>