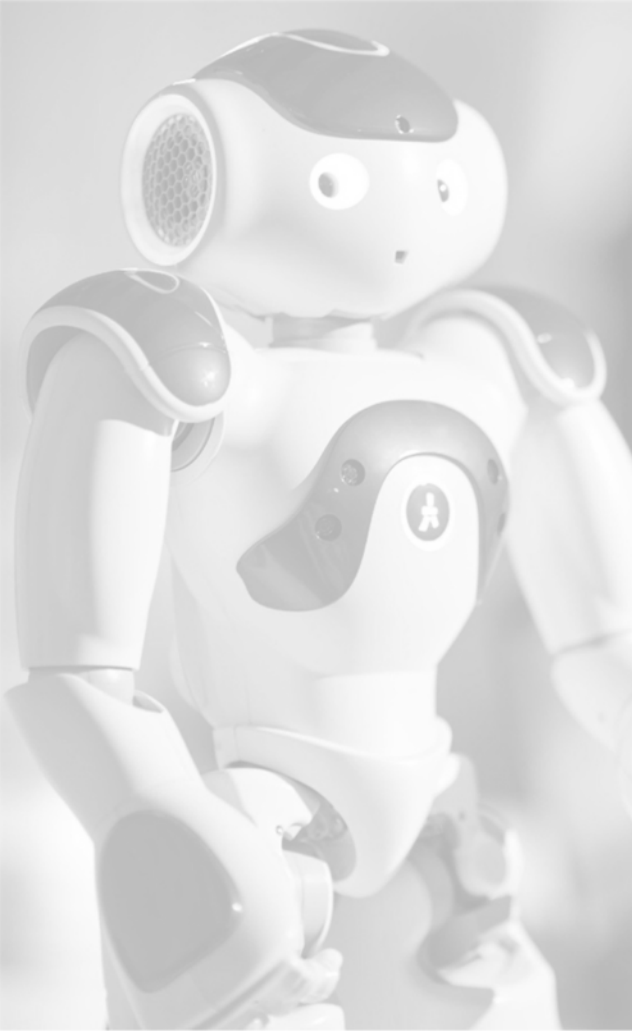
Approaching breaking point?

Global Technology Risk Management Study

April 2019

pwc



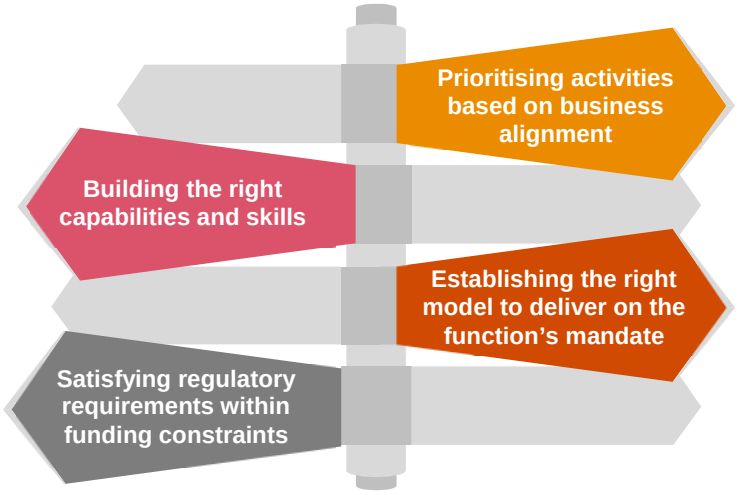
Technology risk management has not kept pace with changing customer expectations and digital strategies. Business functions have fewer resources available but are trying to manage an increased threat landscape and greater regulatory scrutiny. The old model of managing technology risk is no longer sufficient.

Digital strategies are transforming the way organisations are doing business and are disrupting the financial services industry. Business leaders and executives are now awake to the strategic importance of technology and the role that the technology group should be playing in driving the business forward.

This reliance on technology dramatically increases the importance and visibility of the technology risk management function, and highlights the role they must play in delivering a resilient and secure customer experience.

Despite this increased importance, only 51% of our survey respondents noted that their organisations have representation from the technology group at the Board level. It is no surprise then that technology risk management is still not aligned with business objectives and direction.

Technology risk management functions continue to experience significant challenges with:



To deliver truly effective technology risk management, functions must address these issues and establish a vision for a future operating model. The technology risk management function of tomorrow must:

- position itself as a proactive partner who adds value to the organisation;
- establish a clear structure that captures roles and responsibilities to develop the right capabilities; and
- leverage advances in technology to streamline reporting and automate repetitive tasks.

Without establishing and clearly articulating this vision for the future operating model, technology risk management functions will continue to play catch-up and fail to deliver on their mandate, and struggle to provide a robust challenge.

Headline findings from survey respondents

Culture is a barrier to delivering value and becoming a proactive function.

Technology risk management continues to be seen as a cost within the organisation, and functions are struggling to be seen as a value-driving partner. Functions are perceived as fire-fighting, while our study shows a shift in how they want to be viewed. We asked respondents what they wanted the function to be known for, and the top three most common responses were:

1. Being viewed as a proactive risk function
2. Being equipped with a broad skillset
3. Delivering seamless reporting

Diversity in technology risk management continues to be a challenge for organisations and is a barrier to improving function culture. Only 65% of our survey respondents felt their organisation was addressing the balance of women in technology, while a lack of qualified candidates was noted by respondents as the biggest barrier to increasing diversity.

The path to becoming a true value-driving partner for functions starts with delivering critical services in a more proactive and less reactive manner, broadening the talent pool available, and having a sharp focus on “doing the right things” that matter to the organisation.

Regulatory expectations are out-pacing functions.

Regulators globally are now focusing more on non-financial risk than ever before. Regulators in Canada, the UK, the US, the EU, and Asia-Pacific have recently commented heavily on topics linked to technology risk including third party risk management, cybersecurity, and operational resilience.

This trend will likely continue, as will more frequent supervisory inspections. This puts a strain on the time and resources of technology risk management functions to provide full visibility of regulatory requirements and gaps. 75% of respondents in our survey were unclear or unsure whether their organisations had the resources (skills, funding, and technology)

available to meet the increased demands. Additionally, 35% of respondents noted their organisation currently had no function in place to understand and track technology-related regulatory requirements. Despite the increased regulation, it is surprising to see that there has been a reduction in the size of technology risk functions relative to organisation size since our 2016 PwC Leading IT Risk Management Practices Survey.

Functions should leverage available technology and streamline the reporting process, providing clear and readily available data, all the while building capabilities to manage increased and complex requests.

Function structure and alignment of activities is unclear.

While the three lines of defence (3LOD) model is now well established and broadly understood, most organisations continue to face challenges aligning activities, or defining roles and responsibilities across the three lines. Challenges such as duplication of tasks, cumbersome reporting and neglected critical activities continue to exist globally.

76% of respondents noted that the technology risk management function's operating framework did not fully consider engagement and co-ordination with other units within the 3LOD. Further, since our 2016 survey, our respondents noted a drop in the size of the risk functions relative to the size of the organisation.

A clearly defined and articulated set of roles and responsibilities to manage technology risk is critical to provide the highest value to the organisation by focusing on what matters most to the business.

Reporting and monitoring is not adequate to drive challenge.

The previously mentioned increasing regulatory scrutiny, coupled with shortages of available and qualified candidates, highlights the value of a clear and efficient process for reporting and monitoring risks. However only 8% of our survey respondents indicated that they believe that their organisation is highly effective at technology risk reporting and control monitoring.

One of the greatest barriers for technology risk management functions to becoming a value-driving partner is delivering services in a proactive rather than reactive manner. Considering this, only 14% of respondents felt their function was highly effective at identifying future, potential, or emerging risks related to technology.

Reporting of critical risks in an easy-to-understand format, through leveraging technology and based on real-time data, will enable better decision-making and stronger challenge by risk management functions.

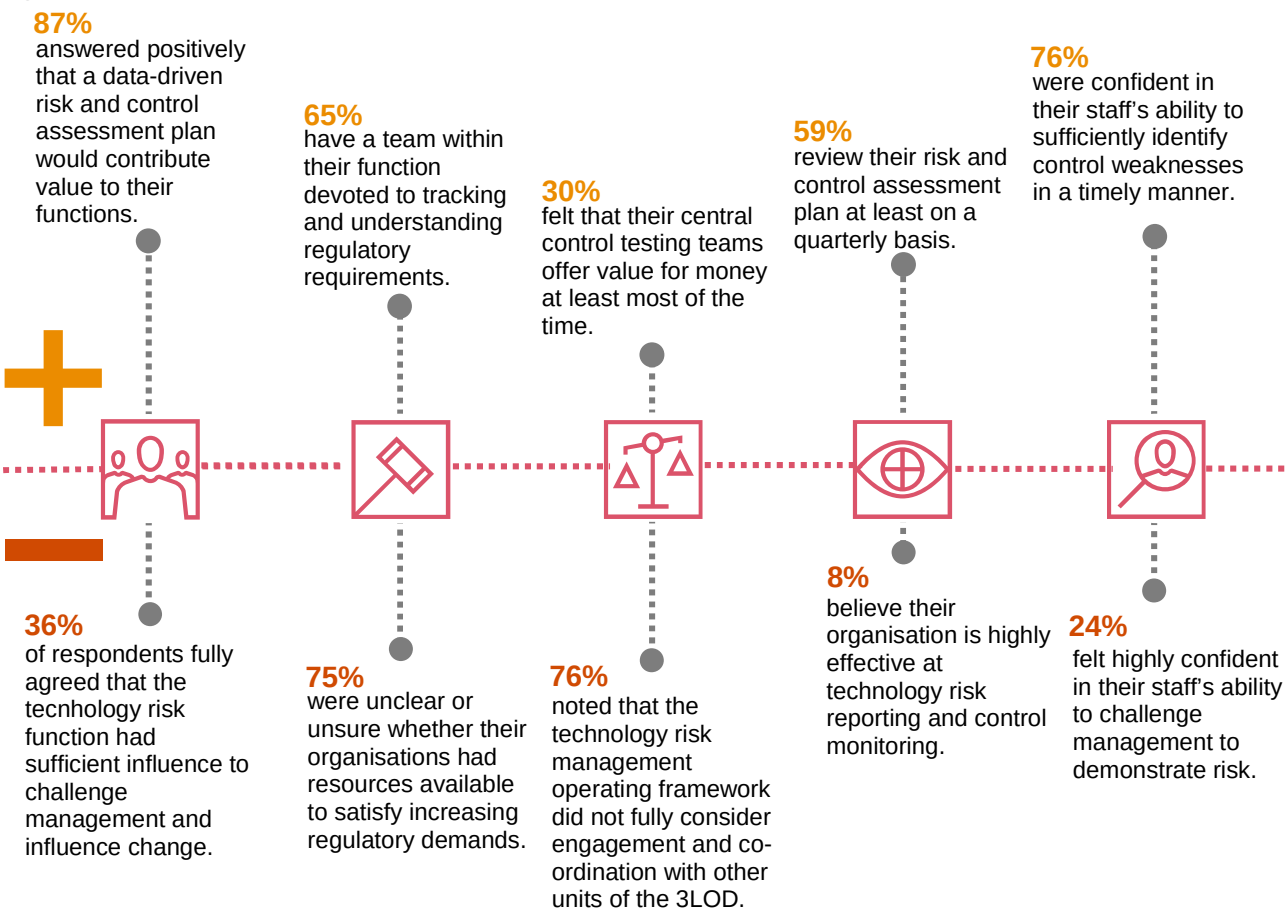
Technology risk management has a clear skills and capabilities gap.

The profile of the technology risk management professional is evolving. Like many other disciplines, a shortage of available and capable candidates continues to be a significant challenge for technology risk management functions, and respondents to the survey noted that developing or acquiring different skills and capabilities to meet emerging requirements was the highest priority to increase the value of the function.

While it is understood that the role is evolving to meet new demands, our survey also highlights challenges organisations are facing with the traditional skillset of a technology risk management professional. Only 30% of respondents noted they were very confident in the skills and capabilities within their function to clearly articulate the impact of technology related issues. To compound this challenge, only 19% of respondents felt highly confident their function had the skills and capabilities to identify control weaknesses in a timely manner.

To meet this challenge head-on, functions should define a professional capability framework; explore new opportunities to identify potential candidates, build new capabilities across the function, and make technology risk a priority across the wider organisation.

Fig. 1

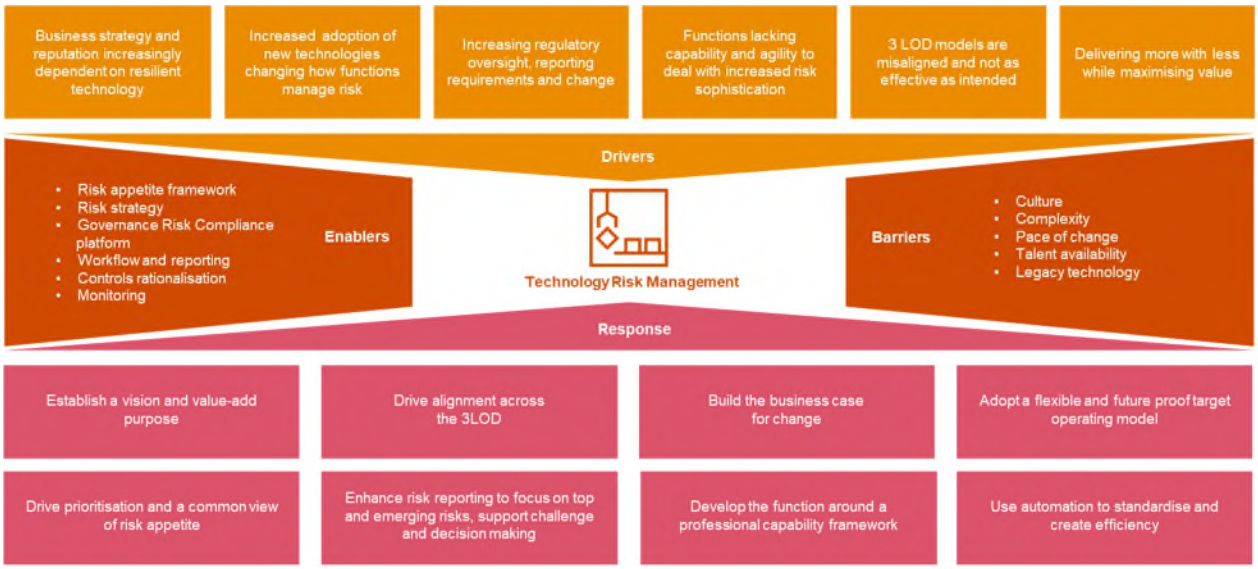


So, what does “good” look like?

Since our 2016 study, we continue to see many of the same challenges existing for technology risk management functions, with new challenges emerging. Functions are being asked to do more; however, resources largely remain the same or have decreased. The reliance on technology to be a business-enabler is only expected to increase in the coming years as the digital delivery model gathers pace and evolves. Likewise, functions are expected to leverage the same innovations in technology to manage risk more effectively and in a proactive manner, while considering the challenges with structure and alignment of activities.

So, what does “good” look like for a technology risk management function? To be better positioned for long-term success, functions need to develop a thoughtful response to these challenges and deliver a robust technology risk program, facilitating resilient technology capable of absorbing shocks or uncertainty. As illustrated in Figure 2, the technology risk management function must also consider the enablers available and the barriers in place that may hinder the success of the mandate.

Fig. 2



Good technology risk management, along with accurate reporting, allows senior management to make informed decisions about risk appetite, target investment in risk remediation where it matters, or accept and manage risk that can facilitate business growth.

Our perspective is that an effective technology risk management function must prioritise the following responses on the journey to building a platform to meet new and existing challenges head-on:

Fig. 3

Our findings

Organisational culture

Firms globally are awake to the impact that culture has on an organisation's ability to meet and exceed its goals, deliver services to customers in a digitally enabled manner, and enhance brand recognition and reputation. The new business model requires organisations to embrace change internally to effectively manage risk.

Establishing a centralised control function within the organisation is an example of a new risks management delivery model to effectively manage technology risk, however study respondents noted that "*organisational culture or resistance to change*" was one of the top five barriers in transitioning to this model.

To drive the organisation forward and effectively manage the technology risks associated with new delivery models, the technology risk management function needs to be seen as a change agent internally. It's concerning then that only 35% of survey respondents fully agreed that the technology risk function has sufficient influence to challenge management and drive positive change.

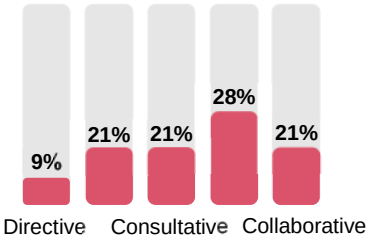
While functions are still demonstrating challenges being seen as change agents internally with sufficient teeth and influence, it was positive to note that functions are now indicating a more collaborative approach to managing risk. When asked to plot themselves along the directive-consultative-collaborative continuum, an encouraging 21% of respondents noted their approach is now collaborative, while a further 28% of respondents put themselves between consultative and collaborative. Perhaps most encouraging of all, only 9% of respondents noted their approach is directive.

Fig. 4

of respondents fully agreed that the IT risk function had sufficient influence to challenge management and drive positive change

Fig. 5

We asked participants how their business and technology teams work together:



A benefit to continuing with this shift from a directive approach to a collaborative one is positioning the function as a proactive team from more traditional reactive risk management methods. When asked to identify which capabilities they would seek to improve to further enhance their reputation as a value-driver, respondents noted that “building or enhancing key risk and control indicators to enable a predictive view of risk” was ranked as the third highest priority. Additionally, 87% of survey respondents answered positively that a live data-driven risk and control assessment plan would further position the function as a value-driver. When asked how effective they believed their organisation was at identifying future potential or emerging risks, only 14% of respondents noted they were highly effective.

Of course it is impossible to discuss workplace culture without talking about diversity. Like many facets of the wider organisation, the technology risk function continues to face challenges identifying, recruiting, and retaining diverse candidates to fill roles. Survey respondents noted a lack of available candidates was the biggest barrier to increasing diversity within their function, while lack of interest by diverse candidates was noted as the second greatest barrier. Further, only 65% of respondents noted they believed their organisation was addressing the balance of women in technology.

Looking to the future, we asked survey respondents what they want the technology risk management function to improve upon. The results were interesting as outlined in Figure 6 below.

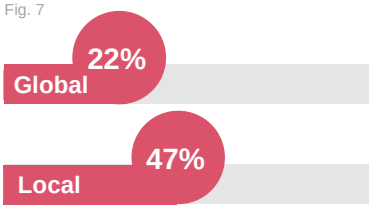
Fig. 6

Our respondents prioritised improving the following capabilities to enhance the value of their technology risk management functions

Changing regulatory environment

In the three years since the 2016 survey, there has been a substantial increase in regulation and inspections. Non-financial regulatory requirements are being elevated to a significant risk for most businesses. The burden of an ever-increasing regulatory environment is also exacerbated by functions being asked to do more, with less.

Fig. 7



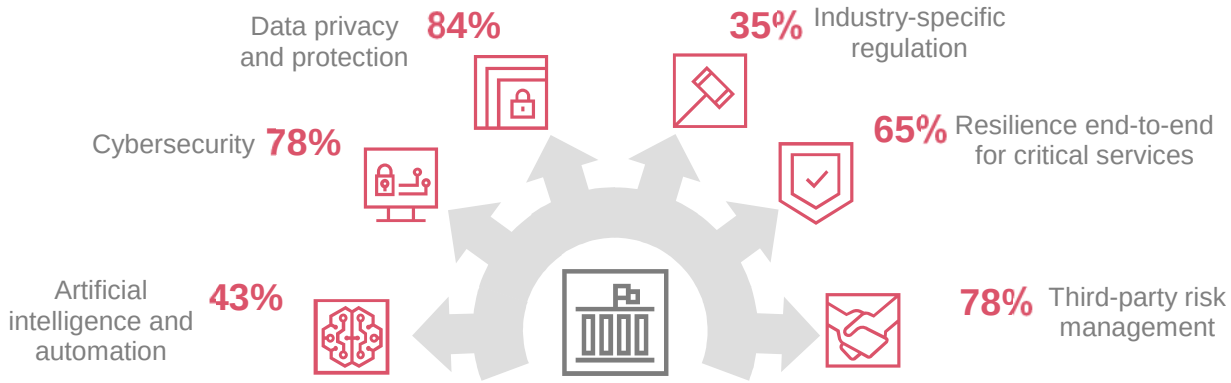
Percentage of respondents who stated that they were very confident in their ability to timely identify new regulations or changes to existing expectations

From global overhauls regarding data privacy to local regulatory catch-up regarding FinTech and Open Banking, the legislative environment is unrecognisable to that of a few years ago as it relates to technology and operational risk, and cybersecurity risk as a subset. Our survey indicates organisations are behind the required curve.

Many organisations are still in their infancy identifying, understanding, and tracking regulatory requirements for technology, with 24% responding they did not have a team to perform this role. Even when organisations do have a specific function, the sharp increase in regulation still means that they struggle to stay up to date with changes. Only 22% of respondents stated they were very confident in being able to identify new, or changes to, global regulatory requirements or expectations.

Fig. 8

Percentage of respondents impacted by increasing regulatory requirements over the past 18 months:



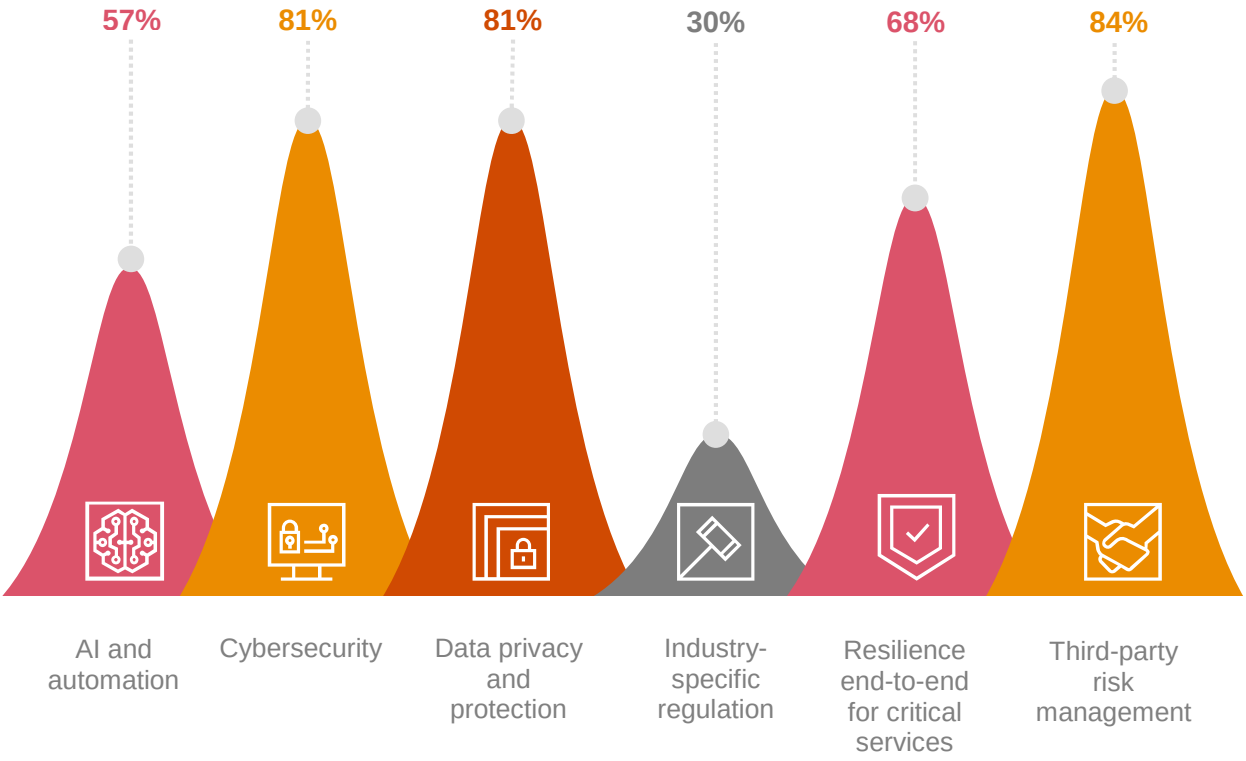
The last year, particularly within Europe, represented significant change with regulators rolling out new guidelines on outsourcing, cybersecurity, privacy, and payments. In addition, the regulators appear to be cracking down on non-compliance, with the UK Financial Conduct Authority publicly stating if “we identify breaches of our rules or principles, we will consider appropriate action, including more detailed investigations into specific firms, individuals or practices”[1] and charging fines just under £300m in the last two years regarding non-financial breaches[2]. This challenge is only likely to be exacerbated with regulation around a post-Brexit Europe looming.

In a similar way, other regulators (including SEC, FRB, APRA, OSFI and EBA) have released significant messages to the market warning around technology risks and are releasing new guidance.

The growth of regulation across Europe, coupled with new releases in Canada, the US, and the Asia-Pac region around information technology is supported by the data collected in our survey. Within the survey, 53% of respondents have been significantly impacted by technology regulatory requirements (including AI, RPAs, cybersecurity, data privacy and protection, third-party risk management, and end-to-end resilience and other specific industry regulators.

Fig. 9

Percentage of respondents who stated that they anticipate regulatory requirements increasing over the next 12-18 months



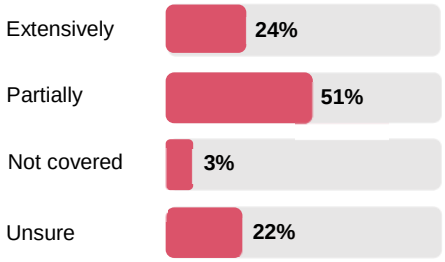
Structure and alignment

In our 2016 study, one of the primary headline findings was that organisations were struggling to define the appropriate operating structure for the 3LOD model, and the division and alignment of tasks between lines (primarily the first and second) was unclear. Fast-forward to 2019 and not much has changed.

When asked to indicate the extent to which their function's operating framework considers engagement and coordination with other lines of defence, just 24% of study respondents noted it was extensive. Similarly, just 38% of respondents noted that the same framework extensively covers function structure, objectivity, and independence.

Fig. 10

We asked respondents to indicate the extent to which their function's documented framework considers cross-line-of-defense-coordination:



Going a level deeper, we continue to see challenges relating to the definition of roles and responsibilities, and how effectively they are established and articulated across the risk function. Despite the maturity of the 3LOD model as an operating framework, only 46% of respondents fully agreed that it has been clearly communicated across the organisation and is well understood, which is fundamental to its effectiveness. Further, 35% of respondents fully agreed that roles that were deemed to be critical for managing technology risk are clearly defined across the organisation. Even within the technology risk function itself, only 32% of respondents fully agreed that the function's mandate, roles, and responsibilities are clear and well understood.

Fig. 11

Only 1 in 3 respondents fully agreed that roles which were deemed to be critical to managing technology risk were clearly defined at their organisations

Functions often fail to fulfill their mandate where roles across the lines of defence or with other risk functions are unclear. Our analysis from the 2016 study identified that there was a clear gap in ownership of risk management activities especially where all lines of defence from the same organisations answered this question. We asked respondents in the 2019 survey to outline which line is responsible for 16 disparate activities.

Based on responses received there still appears to be inconsistency across respondents on who is doing what. 41% of respondents noted that establishing, documenting, and maintaining the IT risk management framework is a First line activity in their organisation, while 38% noted it is a second line activity.

41% of our survey respondents noted that providing training on risk management policies, processes and tools is a first line activity, while 38% noted it is a second line activity. With regards to interfacing with external audit, 38% of respondents noted the primary lead in their organisation was the first line, and 38% noted it as a second line activity. Finally, 38% of respondents noted that technology risk aggregation reporting was a first line activity in their firm, while 41% noted it as a second line activity.

Somewhat more encouragingly, the responses to certain activities demonstrated some better consistency across respondents. For example, our data demonstrated that 70% of participating organisations have tagged the second line to establishing, documenting and maintaining the enterprise risk management framework. In addition, responsibility for both defining, documenting and maintaining the risk taxonomy, and the implementation of GRC tools, seems to broadly sit with the second line, with 65% and 59% of respondents respectively noting both sit with the second line in their organisations.

Fig. 12

Ownership of activities across our respondents' organisations:

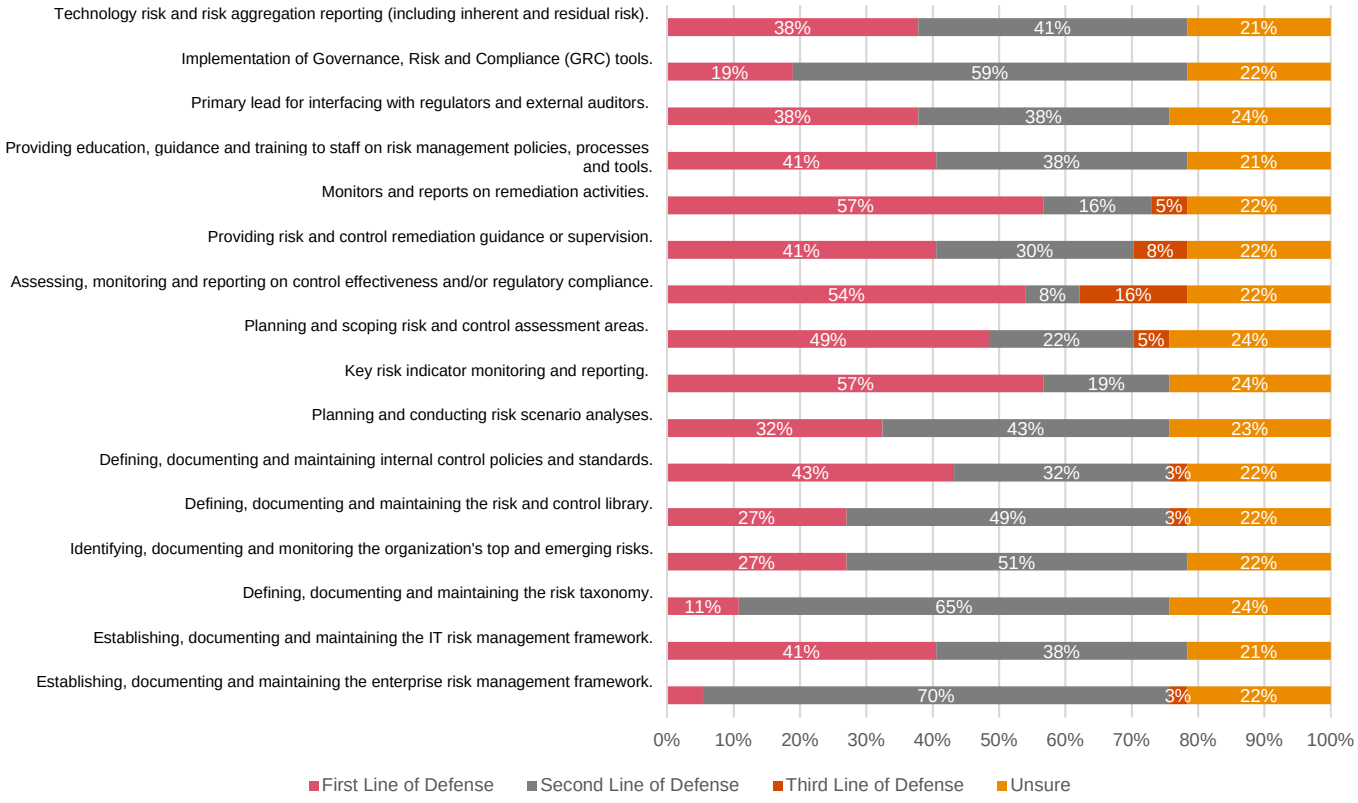
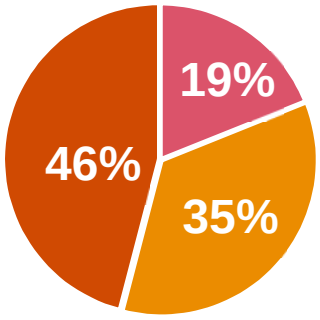


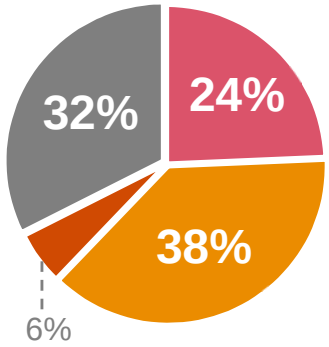
Fig. 13

We asked respondents to indicate the effectiveness of their technology risk reporting functions:

Regulatory reporting



Quarterly board reporting (or similar)



Reporting and monitoring

The role that reporting and monitoring plays in managing technology related risk has never been more important. Unfortunately, our survey suggests that it has also never been more challenging.

There is a noticeable trend upwards in the volume of interested parties from regulatory supervisors, to internal stakeholders. However, only 19% of our survey respondents noted that their regulatory reporting relating to technology risk was very effective, while just 5% of respondents noted the regulatory reporting was very efficient. Internally, while technology risk as a discipline has now garnered increased Board attention, 24% of our survey respondents noted the quarterly (or similar) Board reporting process is very effective, while just 14% noted it was very efficient.

The numbers are alarming. Functions are being asked to report more frequently and in a quicker fashion than ever before, but are clearly struggling to establish a reporting process that is not labour intensive, which strains already limited resources.

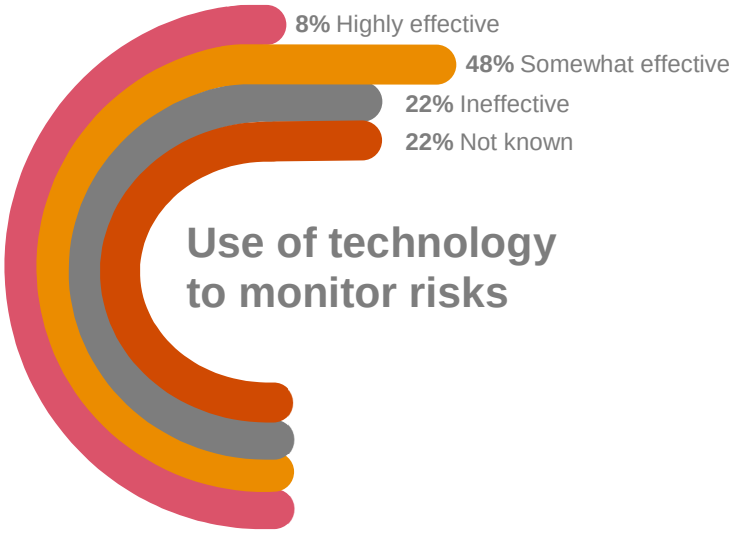
This is further highlighted by respondents outlining that improving the consistency, timeliness and quality of senior management risk and control reporting through data quality, standardisation and automation, as one of the top three capabilities to improve upon in order to increase the value of the function.

Elsewhere in our survey, respondents were asked to rate their function's overall effectiveness for risk management specific activities from "highly" through to "ineffective", and just 8% of respondents rated risk reporting and control monitoring as highly effective. Interestingly and perhaps not unrelated, just 8% of respondents noted that the use of technology for monitoring risks was highly effective.

Developing a risk and control assessment plan is a traditional risk management function activity and more broadly, a mature activity. When asked how frequently assessment plans are reviewed during a year, the results provided by respondents indicate that functions are not clear on how to establish the right cadence or approach. Just 8% of respondents noted that the plan is agreed and locked in once a year only, 22% noted plans are reviewed quarterly but any adjustments to the risk profile are not shared with the relevant technology or business teams, and 38% noted that plans are reviewed quarterly and any adjustments are shared with the relevant stakeholders.

Fig. 14

We asked respondents how effective their organisation was at delivering the following activities:



Skills and capabilities

One of the biggest challenges facing the financial services industry is the depletion of suitably skilled information technology risk specialists. This is also mirrored in our survey as respondents quoted that the number one priority to improve their functions value was to develop or acquire different skills relevant for the changing technology risk landscape. In addition, only 24% of respondents noted that they were highly confident in their staff's ability to challenge management to articulate and demonstrate risk.

Fig. 15

Only 24%

were highly confident in their staff's ability to challenge management to demonstrate risk

There are a number of reasons which have been noted as depleting suitable technology risk resources. In particular a significant increase in the demand for these services as firms look to tap into the value that the top talent can provide an organisation. Others have also suggested that specialised technology firms have a more appealing work-life balance than that of their financial services counterparts.

This is also supported by the figures. New York University Stern School of Business remains the biggest feeder of MBAs into banking among the major U.S business schools, but has seen a significant drop off in recent years. In 2008, 61% of the graduating class sought financial services positions compared to 35% ten years later[3].

Fig. 16

Most demanding areas for risk functions:

1. Cyber-crime and unauthorised access
2. Data privacy and protection
3. Technology governance and culture

The non-financial risk specialist is also finding that they do not need to be that specialised as firms are facing a broader variety of challenges on a day-to-day basis. From the survey responses, we can see that the top three areas that demand the risk function's time and attention are cyber-crime and unauthorised access, data privacy and protection, and technology governance and culture. These are all very distinct categories and will require very different skills. The revelation that teams are stretched to their breaking points is further reflected as organisations answered that only

16% are very confident that their team are able to align existing processes and controls to changing global regulatory requirements. This is further exacerbated by only 24% of organisations being very confident that their team are able to develop new processes and controls to meet changes in regulatory requirements.

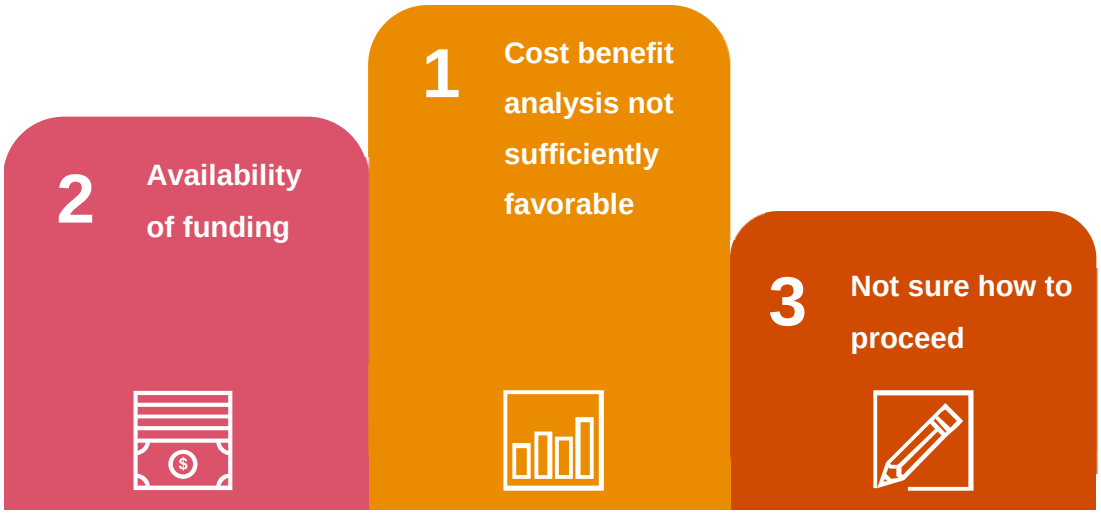
At a high level, management is happy with the staffing of the information technology risk function but feel that they are lacking the specialisms required to deal with some of their most critical tasks. This is supported by the fact that while 76% of respondents were confident that their staff could identify risks and control weaknesses sufficiently and in a timely manner, 11% were not confident in their staff's ability to develop and recommend a pragmatic remediation plan.

Creating a well-staffed and effective risk function in the past year has also proved a challenge. Our respondents stated that the top two barriers to establishing a centralised control testing team was, surprisingly, the cost benefit analysis not being sufficiently favorable and funding constraints. Unsurprising was that the fourth highest ranked reason was around organisational culture or resistance to change, implying that a more agile organisation may find it easier to recruit the right skills.

Another surprise from the data was that the third highest barrier to creating an established control testing team was that respondents were not sure how to proceed.

Fig. 17

We asked respondents what the most common barriers were around establishing a centralised control testing team:



Your global technology risk team

Michael Auret
Partner
C: +1 416 409 6091
E: michael.auret@pwc.com

David Lukeman
Partner
C: +44 7801 227259
E: david.lukeman@pwc.com

Ian Trinder
Director
C: +353 1 792 6000
E: ian.x.trinder@pwc.com

Rizwan Nazir
Director
C: +44 7483 361944
E: rizwan.nazir@pwc.com

Caroline Alleslev-Cserhati
Director
C: +1 416 687 8610
E: caroline.alleslev@pwc.com

Matthew Hunt
Partner
C: +61 3 8603 2399
E: matthew.hunt@pwc.com

Shawn Joseph Connors
Partner
C: +1 (201) 233 2382
E: shawn.joseph.connors@pwc.com

Craig Sydney
Partner
C: +61 2 8266 4938
E: craig.sydney@pwc.com

Noelle Silberbauer
Partner
C: 201 838 4536
E: noelle.silberbauer@pwc.com

Victor Tsui
Director
C: +61 3 8603 2624
E: victor.a.tsui@pwc.com

Our respondents

The 2019 Global Technology Risk Management Study featured responses from companies representing:

- **3 Regions:** North America, Europe, Asia-Pacific
- **5 Financial Services Industry Groups:** Banking, Consumer Finance, Diversified Financial Services, Insurance, IT Services

Thank you to all who participated for sharing your opinions, insights and time.

References

1. https://www.fca.org.uk/publications/multi-firm-reviews/firms-fail-meet-expectations-use-dealing-commission
2. https://www.fca.org.uk/news/news-stories/2018-fines
3. https://news.efinancialcareers.com/ca-en/252381/mba-fintech

Thank you

pwc.com/ca