10-2021

Adopting a risk-intelligent approach to digital transformation: Four traits of digitally mature organisations

Clarence GOH

Gary PAN
Singapore Management University, garypan@smu.edu.sg

Poh Sun SEOW
Singapore Management University, psseow@smu.edu.sg

Yuanto KUSNADI
Singapore Management University, yuantok@smu.edu.sg

Seah Gek CHOO

See next page for additional authors

Citation

GOH, Clarence; PAN, Gary; SEOW, Poh Sun; KUSNADI, Yuanto; CHOO, Seah Gek; and LIM, Cheryl. Adopting a risk-intelligent approach to digital transformation: Four traits of digitally mature organisations. (2021). 1-42.
Available at: https://ink.library.smu.edu.sg/soa_research/1917

Author
Clarence GOH, Gary PAN, Poh Sun SEOW, Yuanto KUSNADI, Seah Gek CHOO, and Cheryl LIM

Joint research by:

Deloitte.

SMU
SINGAPORE MANAGEMENT
UNIVERSITY

ADOPTING A RISK-INTELLIGENT APPROACH TO DIGITAL TRANSFORMATION

Four traits of digitally mature organisations

October 2021

CONTENTS

FOREWORD

In accelerating the digitisation of virtually every industry, the COVID-19 pandemic has generated a newfound appreciation for the benefits of digital transformation, including but not limited to its ability to catalyse new business models, unlock efficiencies, and redefine the very notion of work.

But with the proliferation of digital transformation programmes across organisations, leaders are beginning to understand just how complex these programmes are. Whether they are organisation-wide programmes or taking place in pockets throughout the organisation, digital transformation programmes come with high expectations, tight timelines – and are often fraught with change, uncertainty, and risk.

As digital increasingly becomes a necessity, the conversation is now shifting towards striking the right balance between reaping the benefits that digital transformation offers, and mitigating the risk of potential losses stemming from its insufficient governance, as well as its associated risk and regulatory compliance issues.

To understand how organisations are managing the governance, risk, and compliance (GRC) aspects of their digital transformation programmes, Deloitte Southeast Asia and Singapore Management University (SMU) jointly undertook a set of research in the second and third quarters of 2021. Briefly, the research comprised two components: a survey with board members and executives across a variety of industry sectors in Singapore, and an in-depth, one-on-one conversation conducted with a Singapore-based executive.

What we found was that digitally mature organisations – that is, organisations that report more advanced progress in their digital transformation journeys – display four markedly different traits when it comes to managing the GRC aspects of their digital transformation programmes: they are more likely to recognise the importance of a formal and proactive governance body; regard technological readiness as their weakest governance link; place the ownership of risk identification and monitoring activities with individual business units; and be more acutely aware of the regulatory compliance complexity of their digital transformation programmes.

We hope that you will find this report an insightful read, and look forward to have more conversations with you on the risk-related aspects of digital transformation, and the considerations that you are taking as you navigate your organisations through such programmes.

Seah Gek Choo
Centre for Corporate Governance Leader
Deloitte Southeast Asia

Professor Cheng Qiang
Dean, School of Accountancy
Singapore Management University

MANAGING GRC IN DIGITAL TRANSFORMATION

Our objective is to understand how digitally mature organisations are managing the GRC aspects of their digital transformation programmes, and identify any traits or behaviours that could inform the development of best practices.

RESEARCH METHODOLOGY

Deloitte Southeast Asia, in collaboration with SMU's School of Accountancy Research Centre (SOAR), surveyed 48 Singapore-based executives to understand how they are managing GRC aspects of digital transformation within their organisations. Conducted between the second and third quarters of 2021, the survey covered board member and executive level respondents across a range of different industry sectors (see "Survey respondent demographics").

In the third quarter of 2021, we also conducted an in-depth, one-on-one conversation with a Singapore-based executive to gain more insight into how the organisation is operationalising GRC aspects in their digital transformation programme. The input provided has contributed to the development of our point of view presented in this report.

Survey respondent demographics

Figure 1: Industry sectors

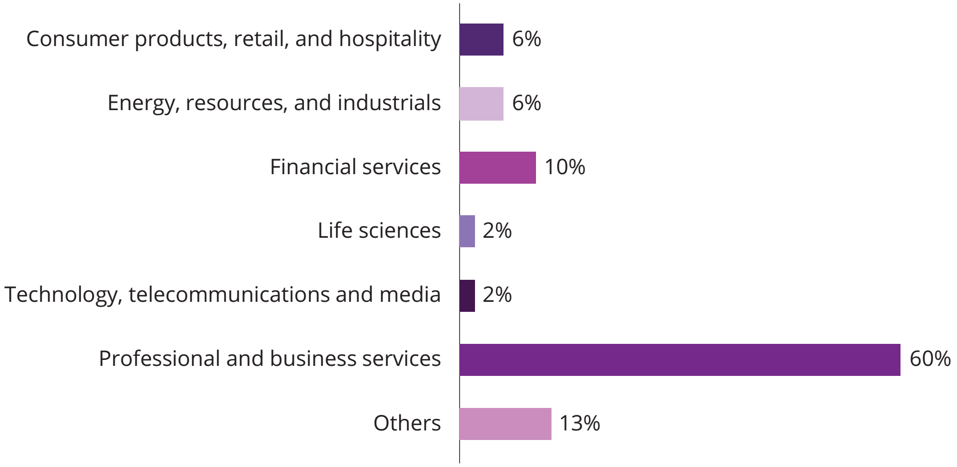


Figure 2: Number of employees in the organisation

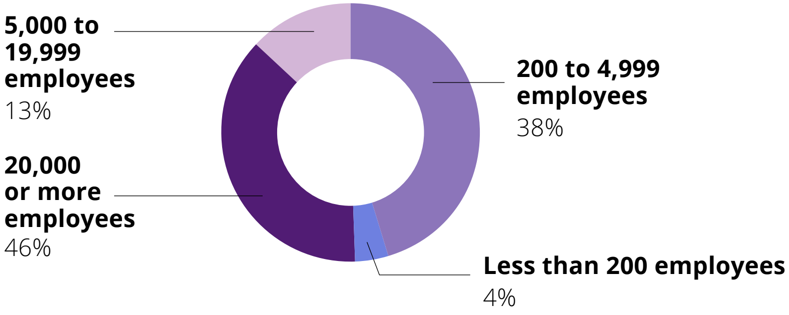
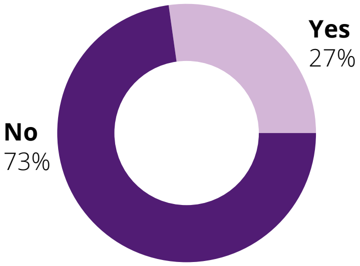


Figure 3: Publicly listed companies



Understanding what digitally mature organisations do differently

Our analysis of the results revealed that survey respondents were evenly distributed across all levels of digital maturity (see Figure 4). A similar observation was made for the four major components of digital maturity: strategy; processes; technology; as well as people and skills (see Figure 5).

Given the wide spectrum of digital maturity levels, we set out to understand how the most digitally mature organisations are managing the GRC aspects of their digital transformation programmes. This would, in turn, enable us to identify the traits or behaviours that could in turn inform the development of best practices.

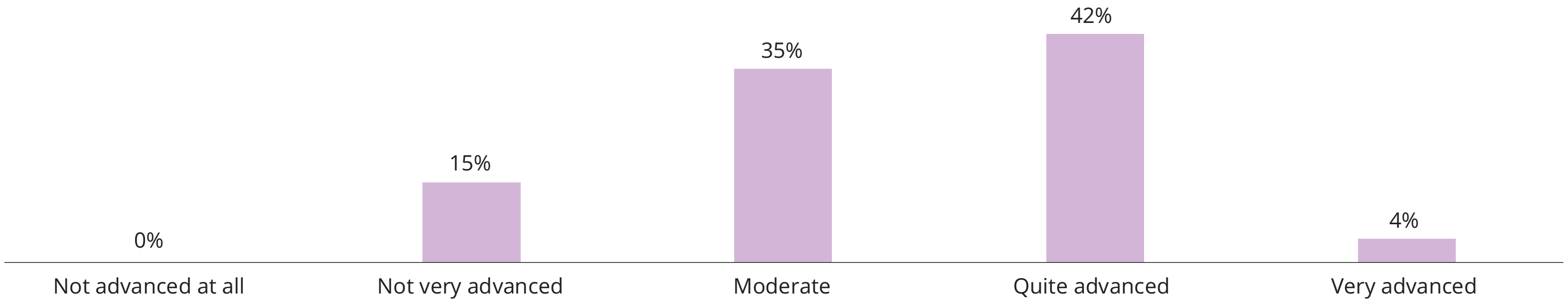
For the purposes of our analysis and discussion, we have segmented the survey respondents into three categories according to their self-reported levels of digital maturity: Leaders, Chasers and Explorers.

LEADERS
Represent the most digitally mature organisations, with survey respondents reporting either very advanced or quite advanced progress in digital transformation

CHASERS
Represent the organisations who are neither the most nor least digitally mature, with survey respondents reporting moderate progress in digital transformation

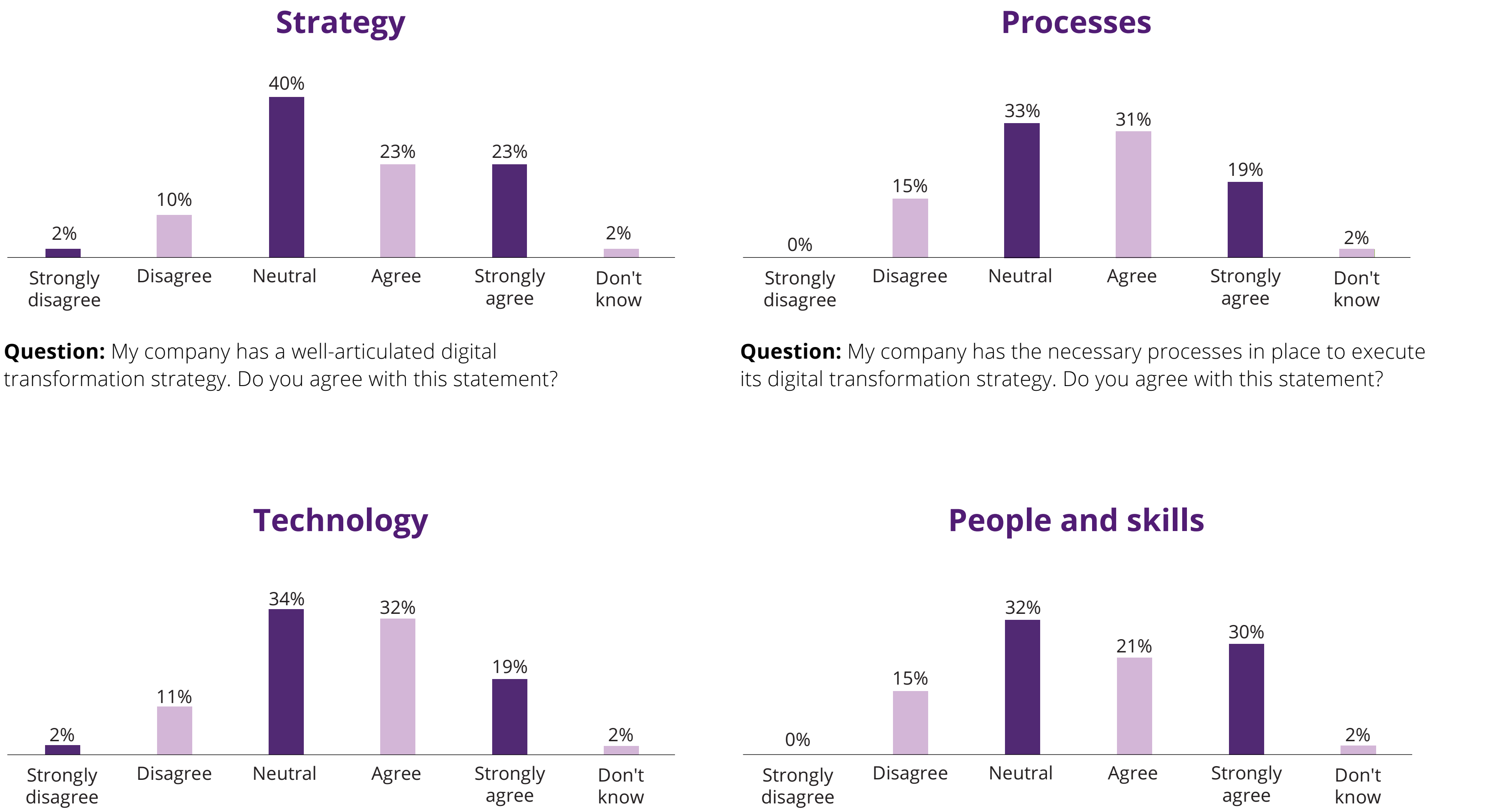
EXPLORERS
Represent the least digitally mature organisations, with survey respondents reporting not very advanced or not advanced at all progress in digital transformation

Figure 4: Survey respondents were evenly distributed across different levels of digital maturity



Question: Overall, how would you rate your company's current progress in digital transformation?

Figure 5: Survey respondents were evenly distributed across different levels of maturity for the four major components of digital maturity



Question: My company has a well-articulated digital transformation strategy. Do you agree with this statement?

Question: My company has the necessary processes in place to execute its digital transformation strategy. Do you agree with this statement?

Question: My company has the necessary technology in place to execute its digital transformation strategy Do you agree with this statement?.

Question: My company has the necessary people and skills in place to execute its digital transformation strategy. Do you agree with this statement?

FOUR TRAITS OF DIGITALLY MATURE ORGANISATIONS

Digitally mature organisations are not only more advanced in their digital transformation journeys, but also display four markedly different traits when it comes to managing the GRC aspects of their digital transformation programmes.

TRAIT#1

Leaders are more likely to recognise the importance of a formal and proactive governance body for digital transformation programmes.

A common pitfall for many organisations embarking on a digital transformation programme is the assumption that the effort should be led by the people closest to the work that is being transformed. But when it comes to governance, closeness to the work may be limiting. Indeed, when individuals are unable to see past the implications on their own business unit or functions, those closest to the work may also pose the greatest risks.

For this reason, having a governance organisational body or committee – one that is a few steps removed from the actual work being done – is vital to ensuring that the benefits of any given digital transformation programme do not outweigh its risks. Ideally, such a governance organisational body or committee should be led by leaders who are not only able to understand the possibilities created by disruptive technologies, but also adept at balancing these against the risks that they create throughout the organisation (see "Emerging role of the Chief Digital Risk Officer").

65% Nearly two-thirds of Leaders report having a formal organisational body or committee

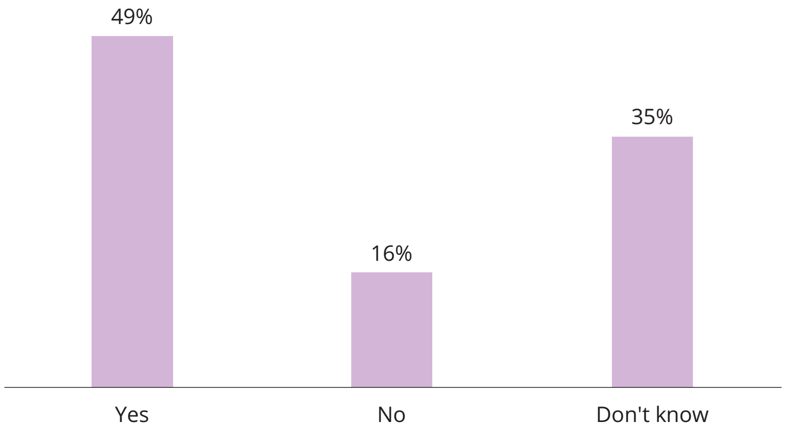
70% More than two-thirds of Leaders report that the organisational body or committee should play a proactive role in the organisation

72% Majority of Leaders report that the organisational body or committee is led by the CEO or CIO

At this point in time, however, it appears that such formal governance bodies or committees are more the exception than the norm (see "When it comes to risk, bigger isn't always better"). Overall, marginally less than half (49%) of our survey respondents indicated that they have a formal organisational body or committee that is responsible for governing digital transformation programmes within their organisation. Indeed, slightly more than half of them (51%) either do not have such an organisational body or committee, or are unaware if such an organisational body or committee exists within their organisation (see Figure 6).

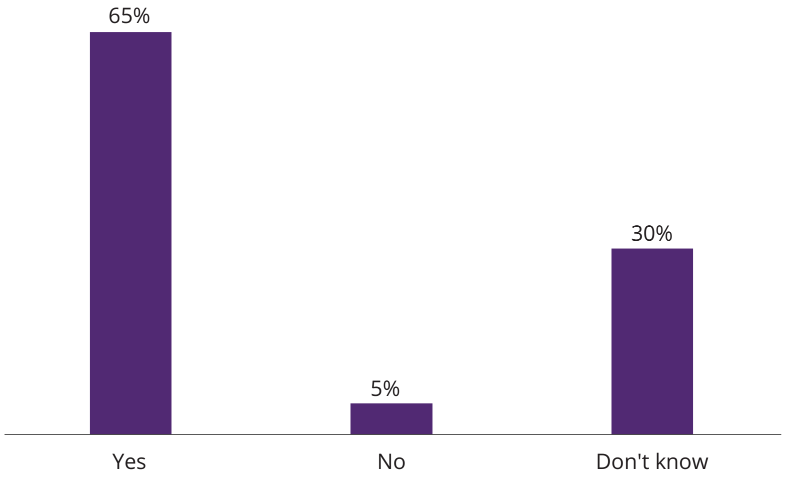
But amongst the digitally mature organisations that have been identified as Leaders, there appears to be a significant, discernible difference. Specifically, nearly two-thirds (65%) of Leaders reported the presence of such a formal organisational body or committee (see Figure 7).

Figure 6: Less than half of survey respondents report having a formal organisational body or committee



Question: My company has a formal organisational body or committee for the governance of digital transformation initiatives. Do you agree with this statement?

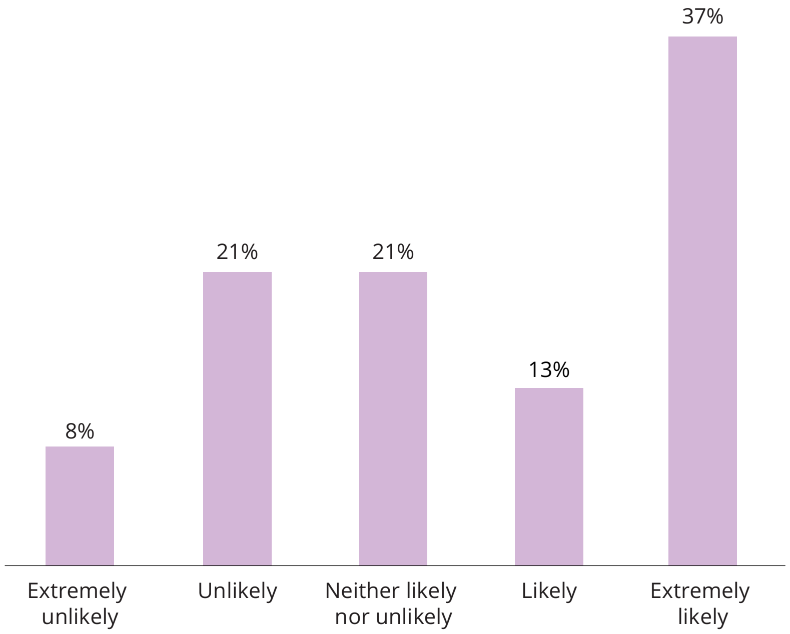
Figure 7: Nearly two-thirds of Leaders report having a formal organisational body or committee



Question: My company has a formal organisational body or committee for the governance of digital transformation initiatives. Do you agree with this statement? (Leaders' responses)

There are some promising signs, however, of a growing recognition of the important role of such a formal body or committee in the governance of a digital transformation programme. Amongst survey respondents who reported not having a formal governance body or committee, half (50%) of them have indicated that their organisations are likely to consider setting one up in the future (see Figure 8).

Figure 8: Half of survey respondents without a formal governance body or committee believe that their organisation is likely to consider setting one up



Question: If your company does not currently have such a body or committee, how likely is it to consider setting one up?

When it comes to risk, bigger isn't always better

Some of the challenges faced by organisations in establishing a formal and proactive governance body were exemplified by the insights shared with us by an internal audit leader at one of Asia Pacific's leading multinational groups.

While the executive clearly recognised the benefits of having a centralised governance body from a risk standpoint, the scale and footprint of the organisation's operations across geographical boundaries made this particularly hard to achieve.

At a high level, senior management is made aware of digital transformation programmes through the usual reporting lines. However, the different jurisdictions conduct their initiatives in a decentralised manner, navigating multiple reporting lines to their own local management and various different boards within the group.

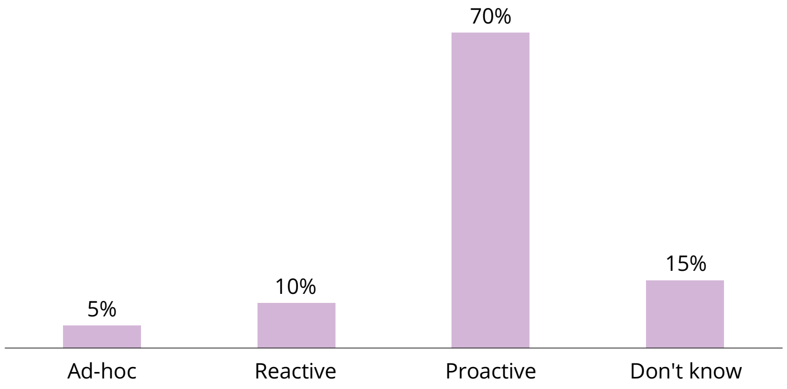
As a result, project workstreams are typically responsible for both the project management and governance aspects of their digital transformation programmes.

Furthermore, while individual business units may propose their return on investments (ROI) metrics for their digital transformation programmes, management does not dictate the scale of the programme – nor subject its business units to any specific targets.

Nevertheless, the mere existence of such a formal organisational body or committee is not sufficient – and the Leaders recognise this. More than two-thirds (70%) of Leaders indicated that the organisational body or committee should play a proactive – rather than a reactive or ad hoc – role in the organisation (see Figure 9).

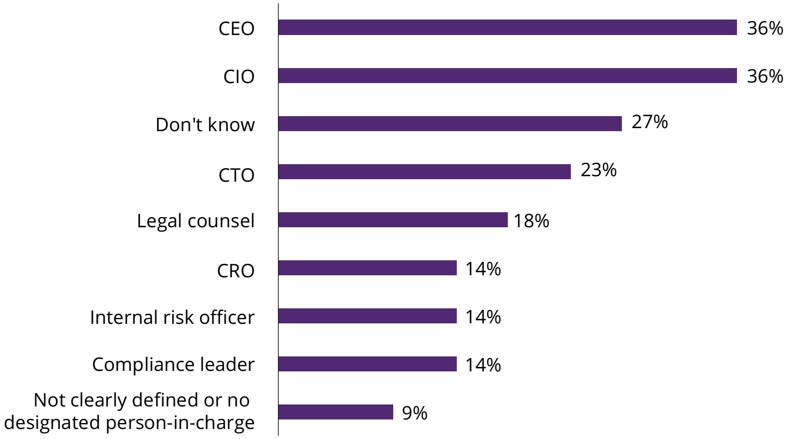
In terms of the overall leadership, majority of Leaders (72%) have also indicated that such organisational body or committees are typically led by either the CEO or CIO at their organisations (see Figure 10).

Figure 9: More than two-thirds of Leaders report that the organisational body or committee should play a proactive role in the organisation



Question: Which of the following best describes the nature of the role that the organisational body or committee plays in the company? (Leaders' responses)

Figure 10: Majority of Leaders report that the organisational body or committee is led by either the CEO or CIO at their organisations



Question: Who is in charge of the organisational body or committee? (Leaders' responses). Respondents may choose more than one option.

To gain a better understanding of how the organisational body or committee functions in practice, we also asked the survey respondents who have reported having such an organisational body or committee to rank from 1 (strongly disagree) to 5 (strongly agree) the extent to which they agree that the organisational committee or body has adequate leadership support; aligns the digital transformation strategy with its strategic plan; reports to top leadership; and guides the risk management programme in relation to digital transformation initiatives.

Across the board, the average scores for all four indicators appeared to be fairly low (see Figure 11). Apart from a slight indifference as to whether the organisational committee or body guides the risk management programme, there is an overall indication that the organisational committee or body does not report to the top leadership – and perhaps as a consequence, does not receive adequate leadership support, and is unable to sufficiently align the digital transformation strategy with the organisation's strategic plan.

Figure 11: Extent to which survey respondents agree with four statements relating to how their organisational body or committee functions in practice

Overall	Average rank
It has adequate leadership support.	2.00
It aligns the company's digital transformation initiatives with its strategy.	2.09
It reports to the top leadership.	2.73
It guides the risk management programme in relation to digital transformation initiatives.	3.18

Question: If your company has a formal organisational body or committee for the governance of digital transformation initiatives, please rank from 1 (strongly disagree) to 5 (strongly agree) the extent to which do you agree with the following statements about the organisational body or committee for the governance of digital transformation in your company.

Emerging role of the Chief Digital Risk Officer

Given the broad impact of digital across many areas of the business, including but not limited to finance, strategy, procurement, as well as organisation design and culture, organisations need to have a clear view of where – and with whom – the responsibility for managing digital risks should lie. But our market observations have revealed that such well-defined roles are rare.

Typically, the responsibility for digital risk is distributed between an organisation's IT, strategy, or risk functions – and led by some combination of the CEO, CIO, CTO, and CRO – or is simply not well-defined at all. As a result, many organisations continue to rely on the 'gut feel' of the individual employees tasked with the project management, as opposed to a structured governance approach.

The good news is that this is beginning to change. In several sectors such as consumer products and financial services, which have traditionally been the earlier adopters of new technologies given their consumer-facing business models, organisations are increasingly appointing Chief Digital Officers to oversee the risk aspects of their digital transformation activities.

While this role may vary according to the specific nature of the business, key responsibilities usually include clearly defining the organisation's risk appetite and overseeing its risk exposures in relation to digital transformation, as well as implementing an enterprise-wide approach to defining digital risk metrics.

TRAIT #2

Leaders are more likely to regard technological readiness as their weakest link in the governance of digital transformation programmes.

As digital transformation programmes inevitably introduce risks to organisations, we asked survey respondents to rank from 1 (largest) to 7 (smallest) the extent to which seven commonly cited digital risks – cyber risk; data security risk; technology risk; strategic risk; compliance and regulatory risk; operational risk; and third-party risk – have increased within their organisations. It is worth noting, however, that these risks are by no means exhaustive: there are at least 10 different identified risks involved in every digital transformation programme (see "The 10 digital risks to watch out for").

Overall, the top three risks that emerged from the ranking were those that are most directly associated with the implementation of technology: cyber risk, data security risk, and technology risk (see Figure 12). However, while Explorers similarly prioritised cyber risk and data security risk, they appear to be more concerned about third-party risk and operational risks than Leaders and Chasers (see Figure 13). One possible reason for this could be a higher reliance on external technology vendors rather than in-house technology teams by Explorers, given their relatively lower levels of digital maturity.

Top three risks identified by Leaders

1. Cyber risk
2. Data security risk
3. Technology risk

Top three weakest governance links identified by Leaders

1. Technological readiness
2. Mindset readiness
3. Multiple decision-making points

Figure 12: Cyber risk, data security risk, and technology risk were the top three overall risks identified by survey respondents

Overall	Average rank
Cyber risk	2.45
Data security risk	3.18
Technology risk	3.53
Strategic risk	4.53
Compliance and regulatory risk	4.68
Operational risk	4.79
Third-party risk	4.84

Question: Digital transformation introduces new risks to a company. Please rank from 1 (largest) to 7 (smallest) the extent to which the following risks have increased in your company.

Figure 13: Different risk prioritisation between Leaders, Chasers, and Explorers

Extent of increase	Leaders	Chasers	Explorers
1	Cyber risk	Cyber risk	Cyber risk
2	Data security risk	Technology risk	Data security risk
3	Technology risk	Data security risk	Third-party risk
4	Compliance and regulatory risk	Strategic risk	Operational risk
5	Operational risk	Compliance and regulatory risk	Technology risk
6	Strategic risk	Third-party risk	Strategic risk
7	Third-party risk	Operational risk	Compliance and regulatory risk

Question: Digital transformation introduces new risks to a company. Please rank from 1 (largest) to 7 (smallest) the extent to which the following risks have increased in your company.

In terms of the effectiveness of their organisations at managing these risks, survey respondents generally consider their organisations to be the most effective at managing the risks that they perceive to have increased the most. Specifically, they felt that their organisations were most effective at managing cyber risk, technology risk, and data security risk, which correspond to their top three identified risks (see Figure 14).

Amongst Explorers, however, there appears to be a greater degree of mismatch between the risks that they perceive to have increased the most and their effectiveness at managing them. Specifically, while third-party and operational risks were identified by Explorers as the risks that have increased the most for their organisations, these risks are also the ones that they consider their organisations to be least effective at managing (see Figure 15).

These findings suggest a significant opportunity for Explorers to recalibrate their risk management efforts to increase the focus on the risks that they perceive to have increased the most. In particular, such organisations should conduct a thorough risk assessment to identify the risks arising from their digital transformation programmes, and use the results to focus their resources on addressing the key risks.

Figure 14: Survey respondents generally consider their organisations to be most effective at managing the risks that they perceive to have increased the most

Overall	Average rank
Cyber risk	2.59
Data security risk	3.46
Technology risk	3.51
Strategic risk	3.82
Compliance and regulatory risk	3.87
Operational risk	5.18
Third-party risk	5.56

Question: Please rank from 1 (extremely effective) to 7 (extremely ineffective) the effectiveness of your company at managing the following risks arising from digital transformation.

Figure 15: Greater degree of mismatch between risks that Explorers perceive to have increased the most and their effectiveness at managing them

Extent of increase	Leaders		Effectiveness at managing
1	Cyber risk	Cyber risk	1
2	Data security risk	Technology risk	2
3	Technology risk	Data security risk	3
4	Compliance and regulatory risk	Strategic risk	4
5	Operational risk	Compliance and regulatory risk	5
6	Strategic risk	Third-party risk	6
7	Third-party risk	Operational risk	7

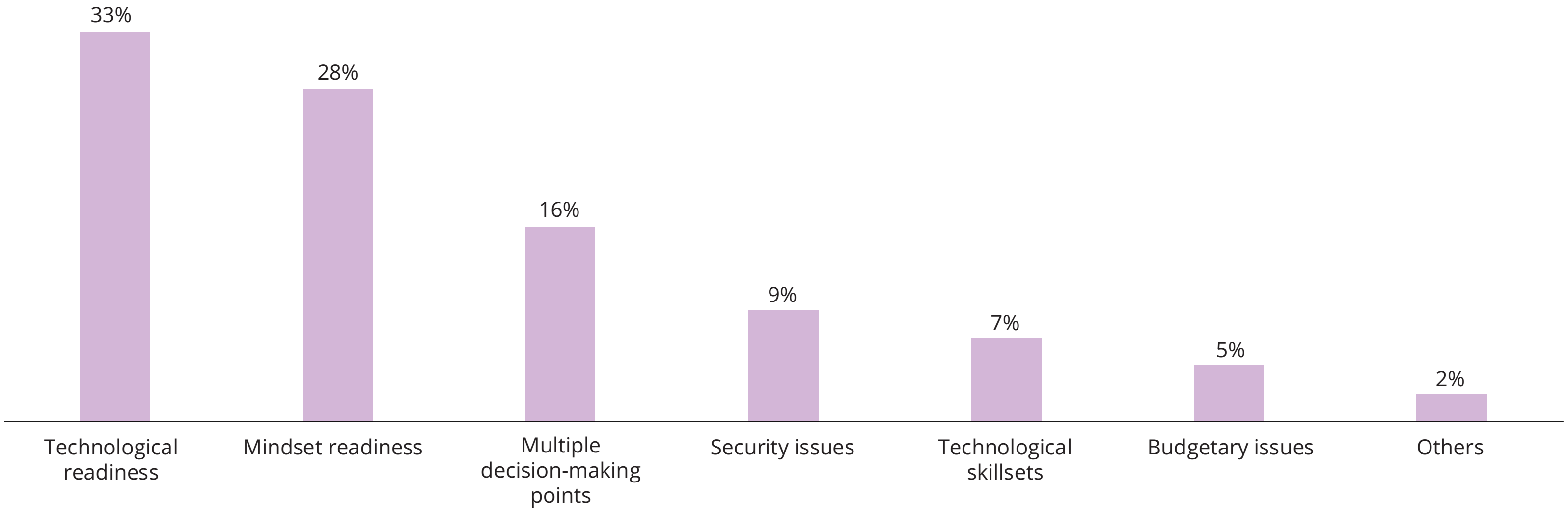
Extent of increase	Chasers		Effectiveness at managing
1	Cyber risk	Cyber risk	1
2	Technology risk	Strategic risk	2
3	Data security risk	Technology risk	3
4	Strategic risk	Data security risk	4
5	Compliance and regulatory risk	Compliance and regulatory risk	5
6	Third-party risk	Operational risk	6
7	Operational risk	Third-party risk	7

Extent of increase	Explorers		Effectiveness at managing
1	Cyber risk	Cyber risk	1
2	Data security risk	Data security risk	2
3	Third-party risk	Compliance and regulatory risk	3
4	Operational risk	Technology risk	4
5	Technology risk	Strategic risk	5
6	Strategic risk	Third-party risk	6
7	Compliance and regulatory risk	Operational risk	7

Question: Digital transformation introduces new risks to a company. Please rank from 1 (largest) to 7 (smallest) the extent to which the following risks have increased in your company.
Question: Please rank from 1 (extremely effective) to 7 (extremely ineffective) the effectiveness of your company at managing the following risks arising from digital transformation.

To understand how COVID-19 has impacted organisations' risk management in the context of digital transformation, we asked survey respondents to identify the weakest governance links in their organisation's digital transformation initiatives during the pandemic. Overall, technological readiness (33%) and mindset readiness (28%) were identified as the top two weakest links (see Figure 16).

Figure 16: Technological readiness and mindset readiness were identified as the top two overall weakest governance links during the COVID-19 pandemic



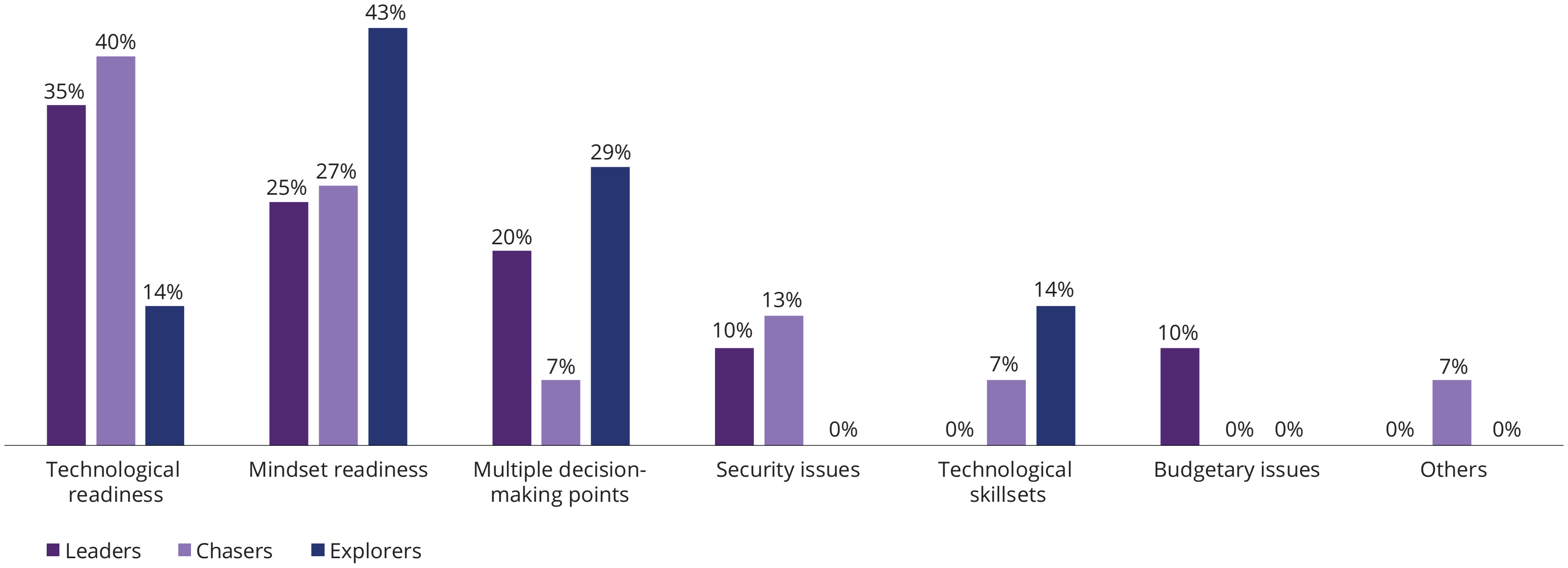
Question: Which is your organisation's weakest link in the governance of digital transformation during the COVID-19 pandemic?

While this is consistent with the observations for Leaders and Chasers, who have both identified technological readiness and mindset readiness as their top two weakest links, Explorers were more concerned with mindset readiness and multiple decision-making points. For the Explorers, technological readiness only came in at a distant third place, along with technological skillsets (see Figure 17).

This finding suggests that structural capabilities, such as the ability to deal with complexity and manage decision-making processes, are basic hygiene factors for the governance a digital transformation programme. It is only when these capabilities are in place that an organisation can move on to consider issues relating to the technology itself.

As organisations accelerate their uptake of emerging technologies and innovation models, the number of new and different types of risks that they will have to manage will only continue to increase and evolve. To ensure that they are prepared to deal with these emerging risks, leaders should therefore focus on developing nimble decision-making structures and an adaptable mindset throughout their organisations (see "New innovation models, new risks").

Figure 17: Leaders and Chasers regard technological readiness as their weakest governance link, but Explorers perceive mindset readiness to be the weakest



Question: Which is your organisation's weakest link in the governance of digital transformation during the COVID-19 pandemic?

New innovation models, new risks

“Every company is a digital company”, goes the adage that executives often cite in their conversations with us – and many do indeed take it seriously. For some leading organisations, digital transformation has become everyone’s responsibility. Across business units and functions, citizen developers – that is, individual employees who leverage drag-and-drop, low-code or no-code applications to create digital applications without the involvement of technology or IT teams – are proliferating.

In such a setup, employees and teams are empowered to design and build their own digital applications, and roll them out quickly in response to business needs. But the drawback is that citizen developers are often not sufficiently aware or knowledgeable about the risks that they are introducing to the organisation by engaging in such activities.

At a real estate company which leverages the extensive use of citizen developers, one executive shared with us how they are mitigating these risks with the introduction of several measures and policies, such as access control limits and risk trainings for citizen developers.

Looking ahead, the executive also believes that teams who are undertaking their own digital transformation programmes should learn to engage with their GRC teams early in the process. By building risk considerations into the design of their programmes, they can reduce the occurrences of future security vulnerabilities, and therefore the need for patchwork maintenance.

The 10 digital risks to watch out for

Although the digital risk profile is unique to each organisation, there are at least 10 different risks that they need to watch out for when embarking on digital transformation programmes:

1

Execution risk
To be successful, digital transformation programmes require fundamental, top-down shifts in how organisations execute. Without those shifts, firms may run into challenges with user adoption, institutional buy-in, and integration with legacy systems. In addition, organisational structures may hamper rather than support agile execution.

2

Cybersecurity risk
As processes and data become more digitised and networked, cybersecurity risk goes up. Firms may exacerbate the risk by trying to protect all digital assets equally rather than shifting more protection to the “crown jewels”. They may also focus on avoidance of cybersecurity incidents at the expense of mitigation strategies, and vigilance at the expense of ease of doing business.

3

Ecosystem risk
Business ecosystems create more opportunities for cyber intrusion and systemic risks. Indeed, an organisation’s weakest link may lie with its partners, vendors, and customers whose systems are closely interfaced with one another., The increased use of partnerships and outsourced services may therefore increase organisational exposure to bad actors, contagion, and errors from model miscalibration. Meanwhile, systemically important technology and data providers can also introduce single points of failure.

4

Emerging technology risk
The greatest digital risks may stem from the technologies that do not even exist yet. Think financial exclusion as technology systems invent their own logic, unintentional collusion as organisations interact through high-speed networks, and breach of fiduciary duty as digital systems take on broader sets of customer-facing responsibilities.

5

Fraud risk
The large majority of fraud is internal, occurring when a current or former employee steals, alters, or destroys business information or assets for personal gain. It may involve also corrupt arrangements involving extortion from or collusion with other individuals, or can involve the falsification of financial or other company records.

6

Privacy risk
Data is proliferating – and so are laws around data privacy and transparency. Between them, these two trends raise the stakes of a data breach involving personally identifiable information.

7

Legal and regulatory risk
Around the world, regulatory regimes are in various stages of maturity when it comes to regulating digital initiatives, and may contradict existing business practices. A rush to comply can sometimes add to the risk by creating complex, overlapping layers of compliance requirements and systems.

8

Brand and reputational risk
Data loss, outages, and misuse can significantly impair an organisation's reputation and stakeholder confidence. Examples include incomplete or unrepresentative data sets, bias in input data, and subconscious developer bias that influences the internal logic of a digital application.

9

Strategic risk
Strategic choices can intensify digital risk. For instance, organisations may opt not to integrate their IT and business strategies. They also may opt to digitise existing processes without improving them or emphasise short-term cost savings over an upgrade of the full digital environment.

10

People and culture risk
Talent to support digital transformation can be in short supply. At the same time, opportunities to upskill or cross-train staff may be limited, and some employees may resist digital transformation for fear of losing their jobs.

TRAIT#3

Leaders are more likely to place the ownership of risk identification and monitoring activities of digital transformation programmes with individual business units.

Despite the unprecedented levels of digital transformation occurring in many industry sectors, the reality is that digital risk remains a largely undefined concept. Typically, organisations tend to be more focused on traditional topical risk areas such as cybersecurity and regulatory compliance. What we believe is needed, however, is a greater end-to-end understanding of the risk implications of digital transformation, which has much broader implications for risk management beyond cyber, data, and regulation.

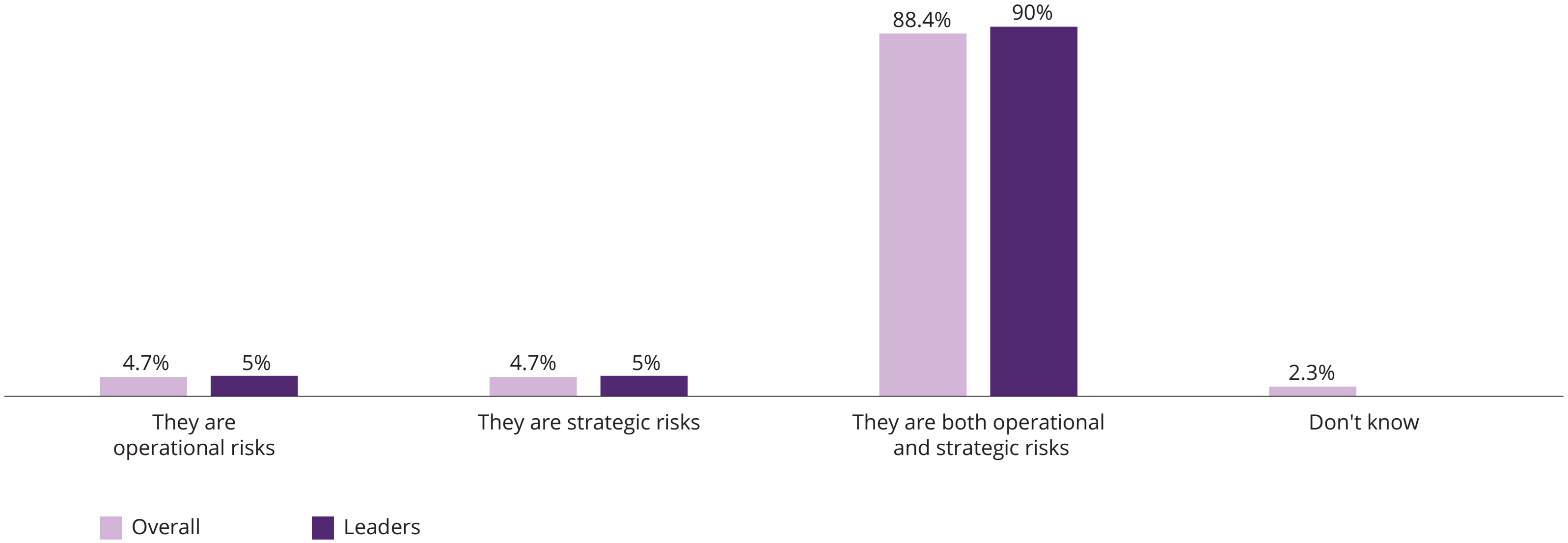
Leaders are more likely to place the ownership of risk identification and monitoring activities with **individual business units (45%)** than with **enterprise risk management functions (40%)**.

45%

40%

As a promising start, we observed that the majority of survey respondents have been able to recognise that the risks associated with digital transformation programmes are both operational and strategic in nature – although this recognition is slightly more pronounced amongst those who have been identified as Leaders (see Figure 18).

Figure 18: Majority of respondents recognise operational and strategic risks associated with digital transformation

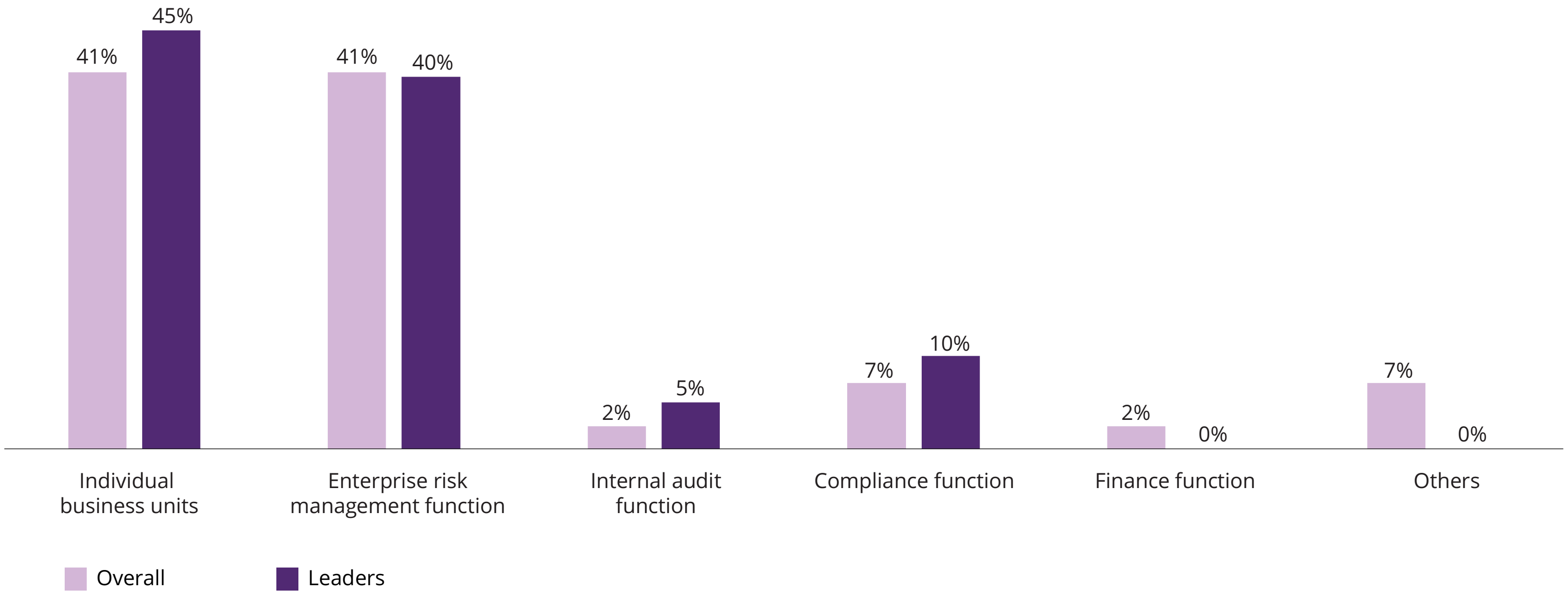


Question: How do you view the risks associated with digital transformation initiatives in governance?

Where Leaders differ, however, is in the ownership of the risk identification and monitoring activities. While individual business units (41%) and enterprise risk management functions (41%) were the two most commonly identified owners for risk identification and monitoring activities across the board, Leaders were more likely to place the ownership of the risk identification and monitoring activities with individual business units (45%) than their enterprise risk management functions (40%) (see Figure 19).

This finding suggests a more risk-intelligent culture within the organisations identified as Leaders, where individual business units bear the primary responsibility for risks originating within their day-to-day operations (see "Creating the risk-intelligent organisation"). In these more mature setups, enterprise risk management, compliance, and internal audit functions – who hold unique roles known as "risk observers" – can then focus fully on their true roles – that is, to provide objective assurance, as well as advise, monitor and report on the effectiveness of the organisation's risk programme to management.

Figure 19: Leaders are more likely to place the ownership of risk identification and monitoring activities with individual business units



Question: Who is responsible for identifying and monitoring the risks in your organisation?

Creating the risk-intelligent organisation

The risk intelligent organisation views risk management not only from the perspective of loss prevention, but also value creation. It acknowledges that risk management must evolve as risks evolve, and pursues the opportunities that risk presents while concurrently managing risks and protecting existing assets. It is insight-driven and action-oriented, and systematically aligns people, process, tools, technologies, and governance into a cohesive system to prioritise and allocate scarce resources to the highest return opportunities.

For most organisations, this represents a departure from how risk has been managed with traditional enterprise risk management approaches. Getting it right requires organisations to take several distinct steps:

1

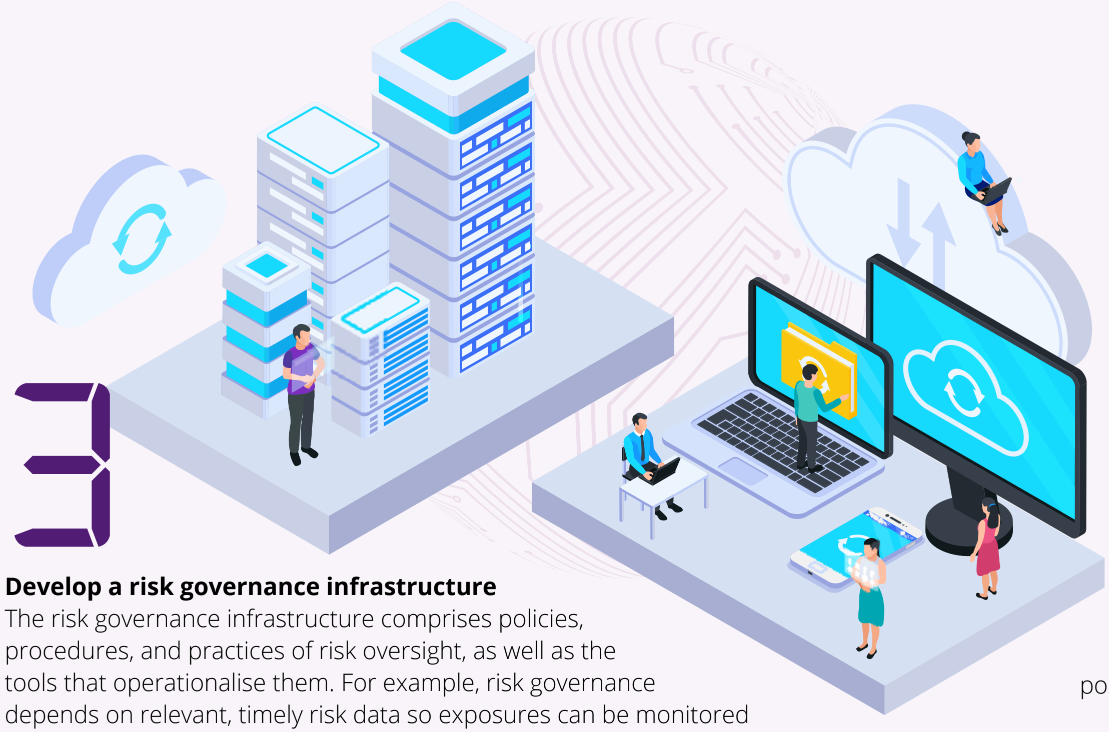
Develop an enterprise-wide view of risks

Risk intelligent risk governance begins with identifying and assessing all risks to the organisation. It then goes on to develop a common language of risk and an enterprise-wide view of risk. Rolling up all risks to the enterprise level enables the Board and management to understand the total exposure of the organisation, within and across risk types, and in all businesses and functions. This process aggregates risks and helps in identifying interrelationships among risks and ways in which risks may amplify one another. For example, operational risks can generate financial risks, which can generate reputational risks – and all of these risks must be recognised and addressed.

2

Assign risk-related roles and responsibilities

Every job function has risks associated with it. The three lines of defence model of risk management and governance can be useful here. In this model, the first line of defence—the business – manages the risks because that is where the risks are located and where they can be managed most effectively. The second line – supporting functions such as compliance, legal, and risk management – helps the first line to define standards, adopt leading practices, connect business leaders across the organisation, and develop relevant tools and mechanisms. The third line – internal audit – provides independent assurance that risks have been identified and management has addressed them. Clearly defined roles and responsibilities are essential to risk governance.



3

Develop a risk governance infrastructure

The risk governance infrastructure comprises policies, procedures, and practices of risk oversight, as well as the tools that operationalise them. For example, risk governance depends on relevant, timely risk data so exposures can be monitored and managed. That data must be communicated to the right people at the right time and in the right ways in order for them to make risk-informed decisions. Clearly defined risk appetite, risk profile, and risk tolerances enable management and first-line teams to understand risk exposures, communicate more clearly about them, and more effectively control them. In addition, the right risk culture – in which the organisation's business strategy and risk strategy, and messaging, conversations, and incentives related to risk are all aligned – can be considered part of this infrastructure.

4

Provide the right resources

Organisations need the right people, processes, and technologies in place to implement and maintain the risk governance infrastructure. People need the requisite expertise and experience to manage the risks within their job functions. Processes for risk management should, to the extent possible, be integrated into operational processes rather than tacked on as check-the-box exercises. That calls for supporting technologies that enable people to identify, monitor, analyse, and manage risks. But policies and procedures cannot implement themselves: senior leaders must provide the resources to enable the organisation to implement them.

TRAIT#4

Leaders are more acutely aware of the regulatory compliance complexity of their digital transformation programmes.

While digital transformation programmes are critical building blocks in enabling organisations to capture new growth opportunities and head off the threat of disruption, the very nature of the emerging technologies that these digital transformation programmes introduce may also create new compliance risks, or add complexity to existing ones.

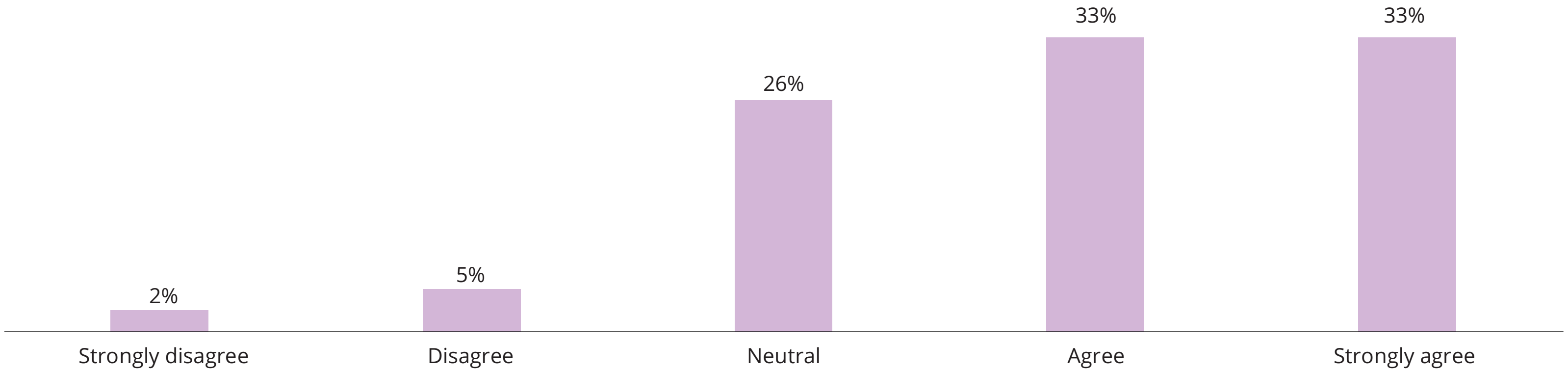
For example, the lack of regulatory clarity on the use of an emerging technology may result in the potential loss of investments and future revenue as new regulations later render existing business models ineffective or infeasible, necessitate frequent changes to business models or operations during a product or service life cycle, or increase the cost of compliance as a result of complex, varying, and sometimes conflicting regulations.

60% Leaders are more likely to perceive **regulatory non-compliance** in relation to digital transformation as a **high** or **extremely high** source of risk

85% However, they also believe that their organisations have managed these aspects **well** or **very well**

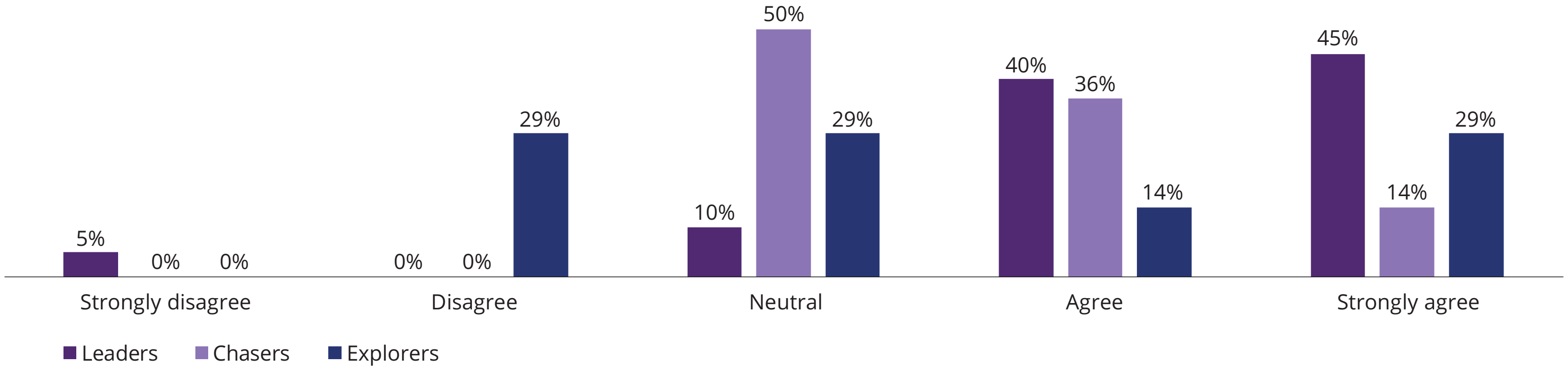
Overall, we found that the majority of survey respondents (66%) either strongly agree or agree that regulatory compliance has become more complex as a result of digital transformation initiatives (see Figure 20). This trend was especially pronounced amongst Leaders, of whom an overwhelming 85% either strongly agree or agree with this statement. In contrast, the majority of Explorers were either neutral or disagreed with this statement (58%) (see Figure 21).

Figure 20: Majority of survey respondents agree that regulatory compliance has become more complex as a result of digital transformation initiatives



Question: Regulatory compliance has become more complex as a result of digital transformation initiatives. Do you agree with this statement?

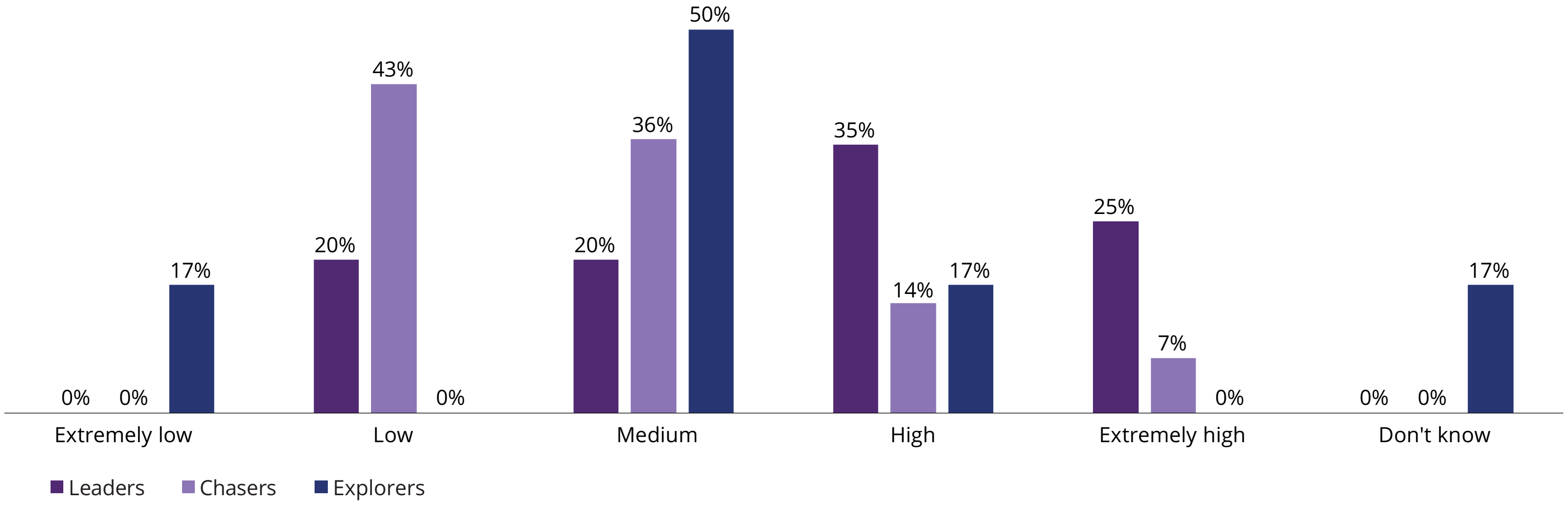
Figure 21: Leaders are more acutely aware of the regulatory compliance complexity of their digital transformation



Question: Regulatory compliance has become more complex as a result of digital transformation initiatives. Do you agree with this statement?

In a similar vein, Leaders were also more inclined to perceive regulatory non-compliance to be posing a high or extremely high risk, with 60% of them expressing this opinion. The majority of Explorers (67%), on the other hand, considered this only to be of medium or extremely low risk (see Figure 22).

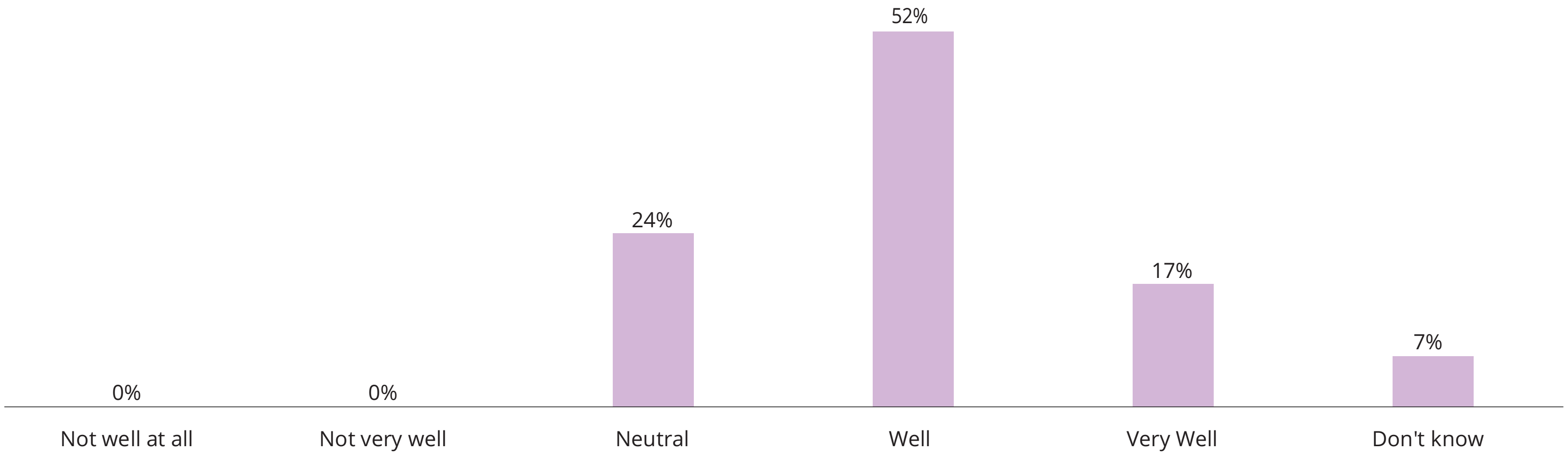
Figure 22: Leaders are more likely to perceive regulatory non-compliance in relation to digital transformation as a high or extremely high source of risk for their organisations



Question: How would you rate regulatory non-compliance in relation to digital transformation initiatives as a source of risk for your company?

Despite the increased complexity of compliance activities in recent years, it is encouraging to see that most organisations appear to be capable of managing the regulatory compliance aspects of their digital transformation programmes. Overall, 69% of survey respondents believe that their organisation has managed the regulatory compliance aspects of their digital transformation programmes well or very well (see Figure 23).

Figure 23: Majority of survey respondents believe that their organisation has managed the regulatory compliance aspects of their digital transformation programmes well or very well



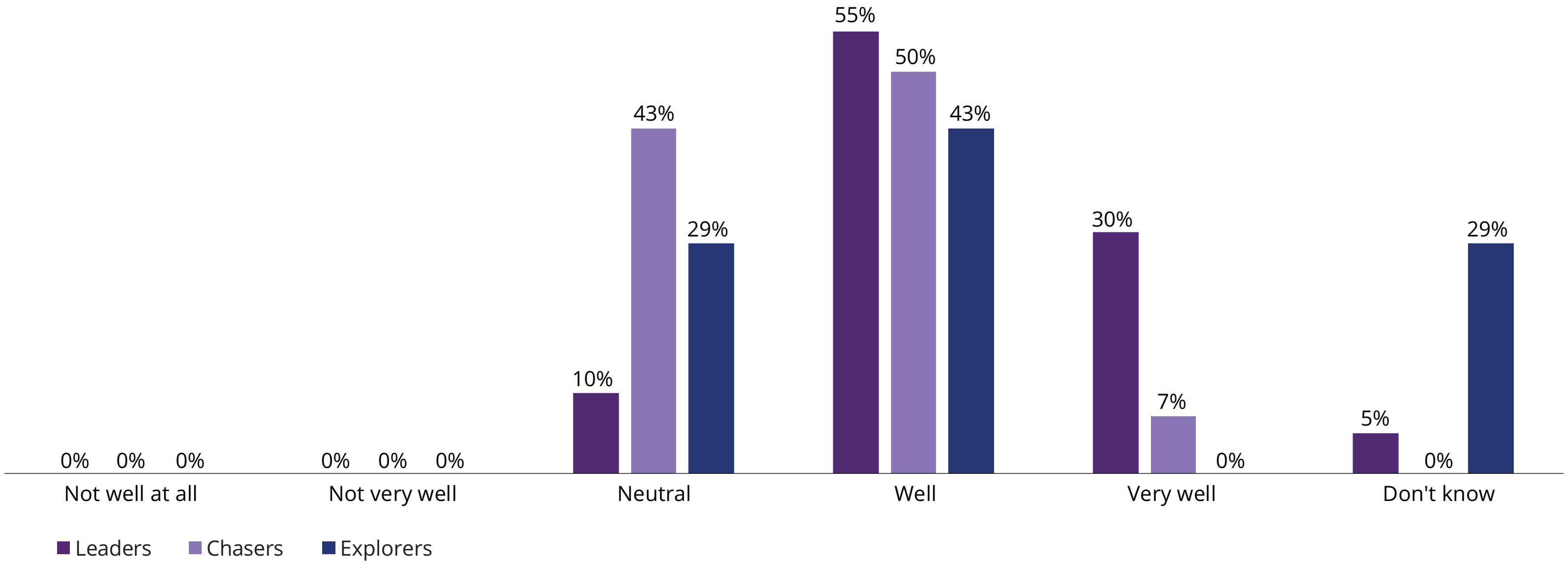
Question: In your view, how has your company managed the regulatory compliance aspects of digital transformation?

This trend is again more pronounced amongst Leaders, of whom 85% share this view. Amongst Explorers, however, the majority (58%) were either neutral or are unaware of how well their organisation have managed the regulatory compliance aspects of their digital transformation programmes (see Figure 24).

One reason for this neutrality or lack of awareness could be due to the differences in the way Leaders and Explorers assign the ownership of risk identification and monitoring activities. As previously discussed, Leaders were more likely to place the primary responsibility for risks with individual business units, whereas Explorers were more likely to place them with their enterprise risk management functions.

With lower visibility on the day-to-day risk monitoring activities, survey respondents within the Explorers category are therefore more likely to be more neutral or less aware of the regulatory compliance implications of their digital transformation programmes.

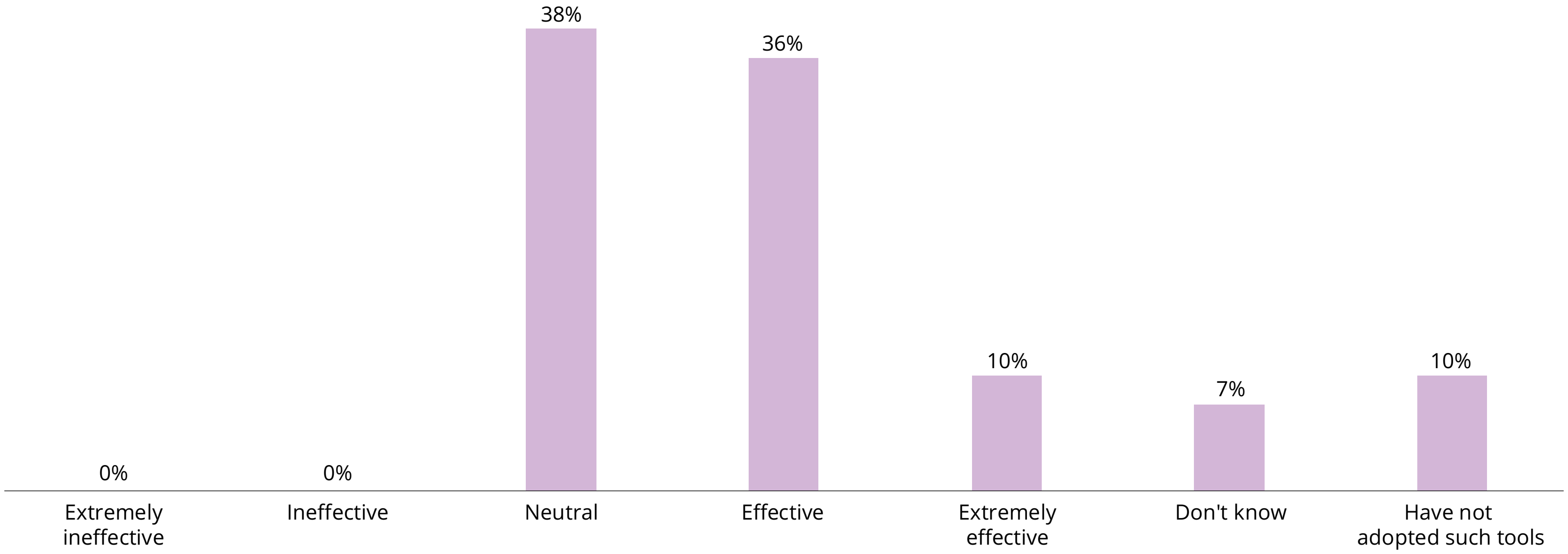
Figure 24: Majority of Leaders believe that their organisations have managed the managed the regulatory compliance aspects of their digital transformation programmes well or very well



Question: In your view, how has your company managed the regulatory compliance aspects of digital transformation?

In terms using regulatory technology tools to support compliance activities, there appears to be significant overall scope for improvement. Specifically, less than half (46%) of survey respondents found such tools to be effective, with the rest either expressing a neutral stance, or indicating that they do not know or have yet to adopt such tools (see Figure 25).

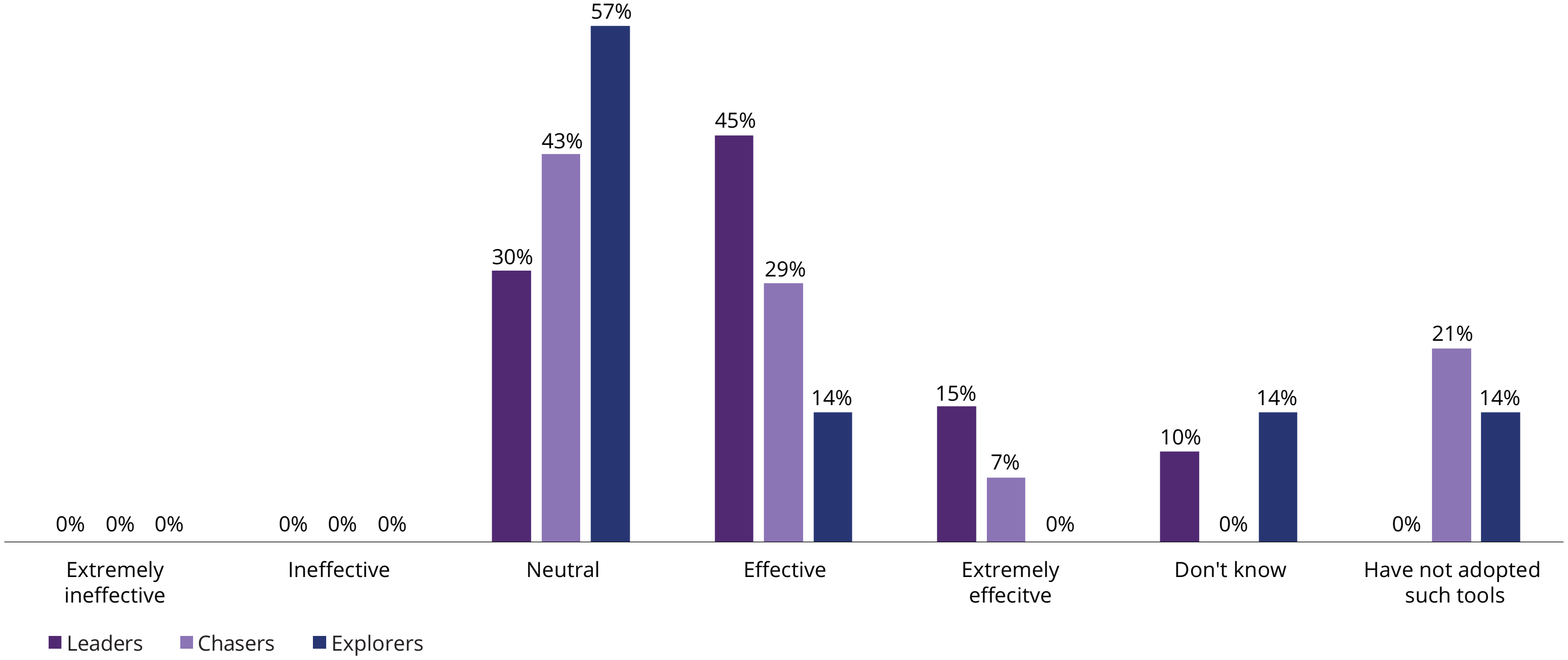
Figure 25: Less than half of survey respondents found the regulatory technology tools that their organisations have adopted to be effective at managing the compliance aspects of digital transformation programmes



Question: How would you rate the effectiveness of the regulatory technology tools that your company adopted to cope with compliance in relation to its digital transformation initiatives?

Amongst Leaders, there are signs of a greater appreciation of the benefits of regulatory technology tools, with a significant majority (60%) of them indicating that such tools are either effective or extremely effective. This is in stark contrast to Explorers, of whom the majority (57%) have taken a neutral stance. In addition, while all Leaders have adopted such tools, a significant proportion of Explorers (28%) and Chasers (21%) either do not know or have yet to adopt these tools (see Figure 26).

Figure 26: Majority of Leaders indicate that the regulatory technology tools that their organisations have adopted have been effective or very effective

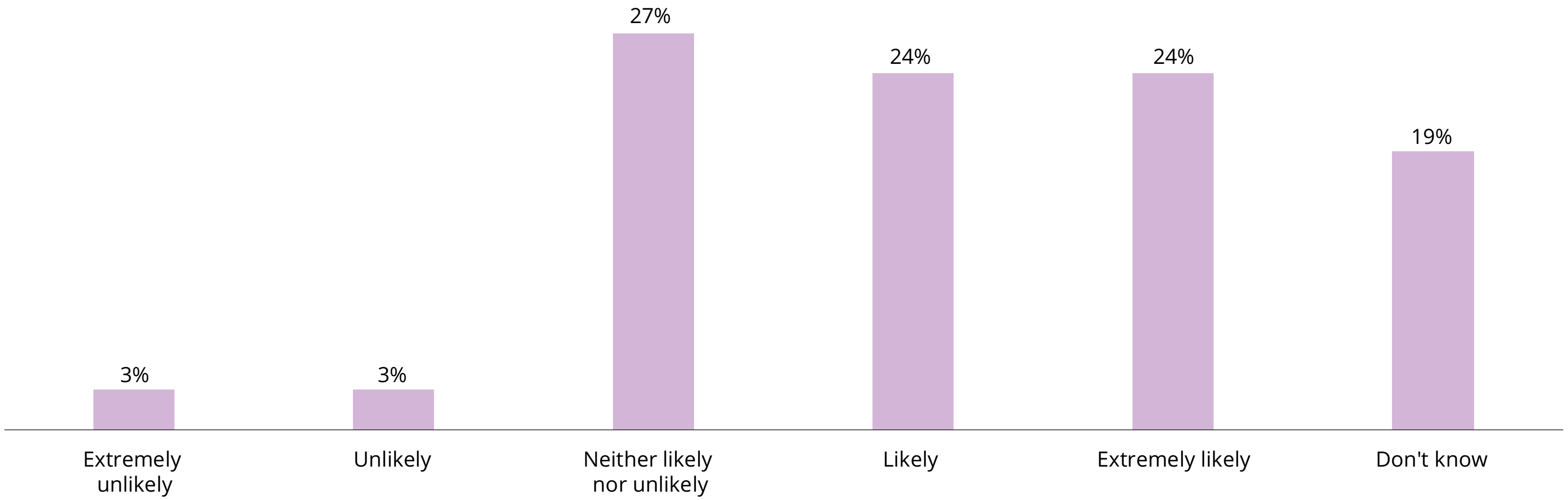


Question: How would you rate the effectiveness of the regulatory technology tools that your company adopted to cope with compliance in relation to its digital transformation initiatives?

Although the majority (48%) of survey respondents whose organisations have yet to adopt regulatory technology tools believe that it is likely or extremely likely that their organisations will consider their adoption, a significant degree of hesitancy can still be observed amongst more than a quarter (27%) of survey respondents, who have adopted a neutral stance towards this issue (see Figure 27).

This is perhaps an unsurprising phenomenon: as is the case with all technology adoption curves, there would always be a group of adopters who would prefer to wait for more successful use cases to proliferate before considering their implementation. To accelerate the adoption of such tools, a greater understanding of their uses and benefits, as well as practical implementation, will therefore be required (see "Turning risks into opportunities").

Figure 27: Majority of survey respondents whose organisations have yet to adopt regulatory technology tools believe that it is likely or extremely likely that their organisations will consider their adoption



Question: If your company has not already adopted regulatory technology tools, how likely is it to consider exploring such tools?

Turning risks into opportunities

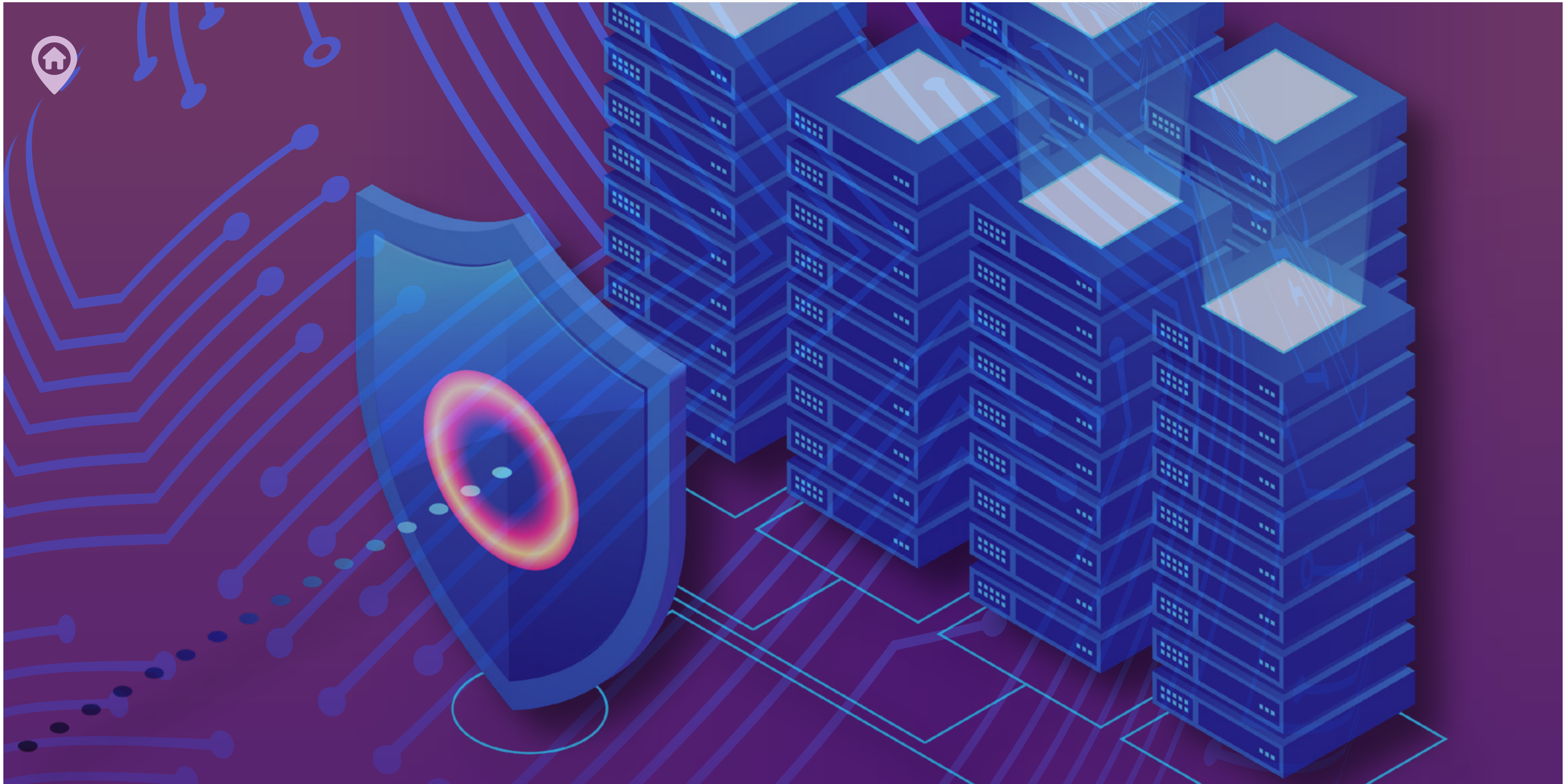
While digital technologies introduce new risks, they can also enhance risk management by enabling new capabilities and unlocking possibilities considered infeasible in the past. By making the right investments in digital technologies, organisations can better manage risk to increase the effectiveness and efficiency of their digital transformation programmes.

But with the proliferation of such technology tools in the market, knowing what to focus on can be daunting. As a start, we propose that organisations consider along the following three key characteristics:

Efficient:
Tools that reduce cost and increase speed in identifying and addressing risk issues. Examples include accelerated identity and access management enabled by robotic process automation; automated regulatory reporting enabled by natural language generation; and accelerated financial close processes enabled by cloud-based workflow tools.

Intelligent:
Tools that improve quality, increase accuracy, and derive richer insights to identify, anticipate, and address risk issues. Examples include augmented detection capabilities through computer vision; simulated crisis management situations in digital reality; and automatic searching of open and deep web sources, watch lists, sanction lists and regulatory sites to perform ongoing due diligence for third parties.

Transformative:
Tools that adopt completely new approach to identifying and addressing risk issues. Examples include cloud-based platforms that enable the sharing of third-party risk assessment data and insights to increase oversight; continuous monitoring of insider threat and reputation risk through predictive analysis of online behaviours; and the use of digital twins to predict faults before they occur.



ADOPTING A RISK-INTELLIGENT APPROACH TO DIGITAL TRANSFORMATION

Even in today's digital and interconnected environment, many organisations continue to exercise risk oversight in siloes that limit management and board's view of risk. But as digital transformation programmes continue to proliferate, organisations must adopt a more risk-intelligent approach to obtain a clear line of sight not only into the risks, but also opportunities that digital transformation presents.

Broadly, a risk-intelligent approach requires central alignment of the specific objectives of the digital transformation programme with the organisation's overall risk strategy. To exercise governance at an enterprise level, organisations should first and foremost consider the implementation of a formal and proactive governance body to oversee all the GRC aspects of any given digital transformation programme. This governance body should also be accountable to the C-suite – although whether they should report directly to the CEO, CIO, CDO, or other executives is a matter of much debate.

As digital transformation becomes table stakes, the irony is also that many of the barriers to achieving true digital transformation are no longer technology related – but pertaining to culture, skillset, execution capability, and the ability to manage risk. This calls for the need to establish protocols to identify, monitor, and communicate about risk at the operating level across the organisation, and ensure that the appropriate risk-related information is in the hands of the right people at the right time.

Just as digital transformation is now everyone's responsibility, risk too must become embedded in organisational culture, and integrated into day-to-day business practices. What organisations need are integrated views of risk, formal risk governance policies, coordinated responses to risk events, as well as tools that enable risk management.

While it is the risk management function's responsibility to develop these enabling tools and facilitate coordination between siloed areas, it is up to the management and board to foster adoption of these views, policies, and processes. Ultimately, it is only with a strong tone-at-the-top that most organisations can stand a chance at adopting a more risk-intelligent approach towards digital transformation.

RESEARCHED AND WRITTEN BY

Deloitte Southeast Asia

Seah Gek Choo
Centre for Corporate Governance Leader

Cheryl Lim
Executive Director, Risk Advisory

Singapore Management University

Clarence Goh
Assistant Professor of Accounting (Practice)

Gary Pan
Professor of Accounting (Education)

Seow Poh Sun
Associate Professor of Accounting (Education)

Yuanto Kusnadi
Associate Professor of Accounting (Education)

CONTACT US

For more insights, please contact

David Chew
Regional Managing Partner, Risk Advisory
Deloitte Southeast Asia
dchew@deloitte.com

Seah Gek Choo
Centre for Corporate Governance Leader
Deloitte Southeast Asia
gseah@deloitte.com

Deloitte. Centre for Corporate Governance

About Deloitte
Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax, and related services. During its 175-year history, our organization has grown tremendously in both scale and capabilities. Deloitte currently has approximately 330,000 people in more than 150 countries and territories, and serves four out of five Fortune Global 500® companies. Yet, our shared culture and mission—to make an impact that matters—remains unchanged. This is evident not only in Deloitte's work for clients, but also in our World*Class* ambition, our World*Climate* initiative and our ALL *IN* diversity and inclusion strategy.

About Deloitte Southeast Asia's Centre for Corporate Governance
Deloitte Southeast Asia's Centre for Corporate Governance (CCG) brings together the knowledge and experience of Deloitte member firms around the world in the critical area of corporate governance. The Centre promotes dialogues with key influencers and business leaders, corporations and their board chairman and members, investors, the accounting profession, academia and government. It also develops advanced thinking on global corporate governance issues such as board oversight of management, director effectiveness, audit committee effectiveness, and executive compensation.

For more information, please contact Deloitte Southeast Asia's Centre for Corporate Governance at **seacentreforcorpgov@deloitte.com**.

SMU SINGAPORE MANAGEMENT UNIVERSITY | School of Accountancy

About Singapore Management University
A premier university in Asia, the Singapore Management University (SMU) is internationally recognised for its world-class research and distinguished teaching. Established in 2000, SMU's mission is to generate leading-edge research with global impact and to produce broad-based, creative and entrepreneurial leaders for the knowledge-based economy. SMU's education is known for its highly interactive, collaborative and project-based approach to learning.

Home to over 11,000 students across undergraduate, postgraduate professional and post-graduate research programmes, SMU, is comprised of six schools: School of Accountancy, Lee Kong Chian School of Business, School of Economics, School of Computing and Information Systems, School of Law, and School of Social Sciences. SMU offers a wide range of bachelors', masters' and PhD degree programmes in the disciplinary areas associated with the six schools, as well as in multidisciplinary combinations of these areas. SMU emphasises rigorous, high-impact, multi- and interdisciplinary research that addresses Asian issues of global relevance. SMU faculty members collaborate with leading international researchers and universities around the world, as well as with partners in the business community and public sector. SMU's city campus is a modern facility located in the heart of downtown Singapore, fostering strategic linkages with business, government and the wider community. https://www.smu.edu.sg/

About SMU School of Accountancy
Established in 2001 as the second school in the Singapore Management University (SMU), the School of Accountancy (SoA) offers the distinctive programmes; the Bachelor of Accountancy, Master of Professional Accounting, Master of Science in Accounting (Data & Analytics), SMU-Tsinghua Master of Science in CFO Leadership, SMU-Zhejiang Doctor of Business Administration (Accounting and Finance) and PhD in Accounting. SoA pursues excellence by offering academic programmes that are responding to the needs of accounting and finance professionals. In particular, its Bachelor of Accountancy programme enjoys recognition from 11 professional and accreditation bodies. SoA continues to receive international recognition for its research strength.

In 2021, SoA is ranked first in Asia and second in the world for archival research in all accounting areas in the Brigham Young University (BYU) accounting research rankings. The achievement is a strong testament to the commitment of SMU faculty towards developing high quality accounting research and placing SoA as a global leader among accounting schools in renowned universities. https://accountancy.smu.edu.sg/

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.