KPMG

Guardians of trust

Who is responsible for trusted analytics in the digital age?

KPMG International
Data & Analytics

kpmg.com/guardiansoftrust

Contents

Foreword

Data breaches. Machine-based decisions. The rise of the robots.

Amid fears and uncertainties in the digital age, the value of trust in a business cannot be overstated. Today, that trust relates not only to a company's brand, products, services and people — but also to the data and analytics (D&A) that are powering its technology.

However, KPMG International research shows that companies are struggling to build this trust.

In the recent *Guardians of trust* study, KPMG International commissioned Forrester Consulting to survey almost 2,200 global information technology (IT) and business decision makers involved in strategy for data initiatives. The survey found that just 35 percent of them have a high level of trust in their own organization's analytics.

At a time when machines are working in parallel with people, this study points to a clear need for proactive governance of analytics in order to build trust.

But who should be responsible for trusted analytics? And what does good governance look like? As organizations undergo digital transformation, with artificial intelligence (AI) sweeping through almost every industry, is someone taking responsibility for the quality, effectiveness, integrity and resilience of D&A?

In the following report, we identify some emerging principles as well as some worrying opinions. The report summarizes the research findings, discussions with industry leaders who are making strides in building trust, and the recommendations and observations on the governance of analytics.

On behalf of KPMG International, I thank the senior executives who participated in the research and interviews. Your candor, transparency and ideas have been invaluable in helping lead the way towards greater trust between people and machines.

To discuss the issues raised in this report or to join us in the effort to bridge the trust gap, please contact your local KPMG office or any of the authors listed at the back of this report.

Dr. Thomas Erwin

Global Head of KPMG Lighthouse
Center of Excellence for Data
& Analytics and Intelligent
Automation
Partner, KPMG in Germany

At a time when machines are working in parallel with people, this study points to a clear need for proactive governance of analytics in order to build trust.

Summary

A trusted organization has traditionally been anchored by the behaviors and decisions of trusted people. As people give way to machines, a trusted organization (and a trusted platform) also requires trusted data and analytics.

KPMG International's *Guardians of trust* report looks closely at the intimate relationship between trust and digital transformation within an organization — who is responsible for ensuring trusted analytics and what good governance can look like in a digital world.

Trust in analytics is lacking*

Only 35% of respondents say they have a high level of trust in their own organization's use of different types of analytics

and 25% admit that they either have limited trust or active distrust.

Trust in an age of digital transformation*

Trust is becoming a defining factor of an organization's success or failure. Underpinning a company's license to operate effectively, trust reduces uncertainty and builds resilience as well as:

influences reputation

drives customer satisfaction and loyalty

inspires employees

enables global markets to function

Executives and customers are wary of technology

Rapid, uncertain tech disruption can lead to unstable levels of internal and public confidence.

Trust in a digital world

The need for trust is expanding from trust in brands, organizations and their employees to also include trust in machines, algorithms and analytics.

The trust gap grows: C-suite executives question the trustworthiness of data, analytics and intelligent automation*

Few decision makers trust the way their organization uses different types of analytics. But the trust gap is not reducing with experience or time.

92% are worried about the impact on reputation

Understanding that trust in analytics is founded on four key anchors

Quality

Effectiveness

Trust

Resilience

Integrity

Trusted analytics is not a vague concept or theory. At its core are rigorous strategies and processes that aim to maximize trust.
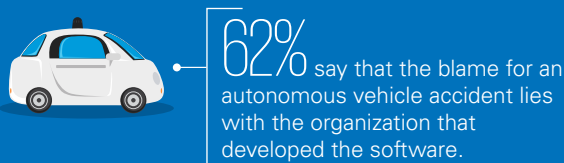
Levels of trust vary by geography*

The trust gap is not the same in every country and decision makers may need to adjust their approach depending on the market they are in.
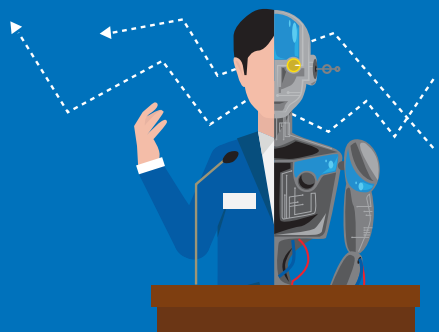
65%   21%

high levels of trust in India vs US
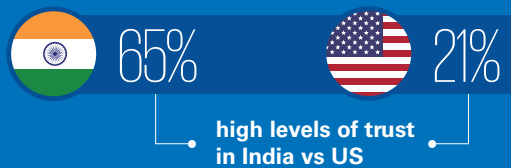
Spreading the blame*

Everyone should share some level of responsibility and accountability for faulty or untrustworthy analytics.

62% say that the blame for an autonomous vehicle accident lies with the organization that developed the software.

Like human, like machine

The governance of machines should not be fundamentally different from the governance of humans.

Creating the foundation

There are eight areas that form the basis for emerging standards, enablers and controls for trusted analytics.

Governance

Processes

Regulation

Data

People & culture

Technology

Strategic alignment

Alliances and supplier networks

Who holds organizational responsibility?*

It is not clear who **within** the organization has primary responsibility for ensuring the trustworthiness and accuracy of advanced analytics and models. A larger percentage says it rests with the technology function.

Key takeaways

If you can't measure it, you can't manage it

Prioritize risks

Create trust-impact personas

Create a buddy system

Stay legal

Checklist manifesto for data and analytics

Don't let the board off the hook

Be flexible with horses for courses

Create a mesh governance framework

* Source: A commissioned study conducted by Forrester Consulting on behalf of KPMG International, July 2017

Trust in an age of digital transformation

Trust is a defining factor in an organization's success or failure. Indeed, trust underpins reputation, customer satisfaction, loyalty and other intangible assets, which now represent nearly 85 percent of the total value of companies in the S&P 500[1], compared with tangible assets such as bricks and mortar. Trust also can inspire employees, enables global markets to function, reduces uncertainty and builds resilience.

It is no wonder that in the KPMG International *Disrupt and grow 2017 Global CEO Outlook* survey, 61 percent of nearly 1,300 chief executives said that building trust among customers and other external stakeholders is a 'top three' priority for their organization. Almost three-quarters said their organization is now placing a greater importance on trust, values and culture in order to sustain their long-term future.

Organizations are also making unprecedented investments in new technologies. KPMG professionals are seeing mass experimentation and uptake in industries from banking and insurance to telecommunications, healthcare, manufacturing and travel. Disruptors are leveraging data, sophisticated analytics, robotics and, increasingly, artificial intelligence (AI) to create new value propositions and business models.

The age of AI also offers new ways of protecting public trust as we shift from humans towards machines. In audit, for example, cognitive systems can analyze millions of records and identify patterns to create more insights on a company's processes, controls and reporting. Algorithms, meanwhile, can be designed to reduce human biases in decision making, and blockchain can offer greater data security and new distributed trust models.

Figure 1
Trust influences corporate reputations and drives customer satisfaction
Building greater trust among external stakeholders and customers is among the top three priorities of my organization today.
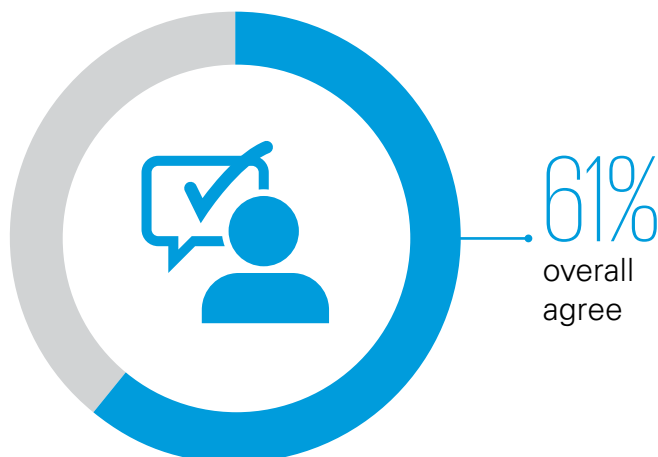
61%
overall agree

The widespread use of AI will make it imperative — and more difficult — to ensure trusted analytics.

Source: 2017 Global CEO Outlook, KPMG International

Trust inspires employees, enables
global markets to function, reduces
uncertainty and builds resilience.

From hype to humble reality

In a high-speed, highly digitized world, trust that has taken years to build can be destroyed almost instantly. Amid the rise of machines, organizations require trust not only in their brands and people but also in their data and analytics. Getting this right is not something that any enterprise can claim to have mastered.

Not surprisingly, some of those who manage analytics and automation are concerned about the risks. The *Guardians of trust* survey questioned 2,190 global senior business decision makers involved in setting direction for data and analytics from nine countries. Ninety-two percent admitted they are worried about the reputational damage that inappropriate use of analytics could cause for their organization.

Figure 2
The impact of analytics on corporate reputation
How concerned are you about the following consequence if your organization's data and analytics models do not work as intended or are inappropriately used?
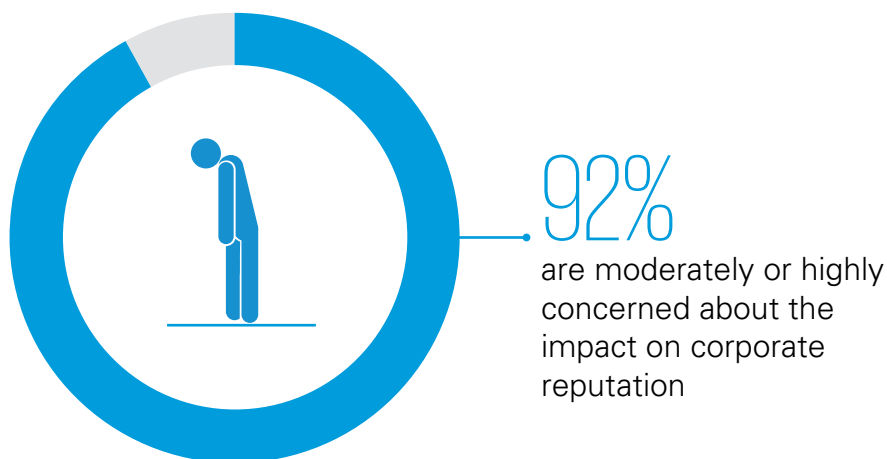
92%

are moderately or highly concerned about the impact on corporate reputation

Base: 2,190 global IT and business decision makers with involvement in setting strategy for data initiatives at their organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of KPMG International, July 2017

Against this backdrop, C-suite executives are starting to ask difficult questions about the trustworthiness of data, analytics and intelligent automation.

What types of governance frameworks and controls are required when the risk-takers are machines, not humans?

How can decision makers trust the insights they are receiving when they don't own the source data?

How would we know if something has gone wrong, and how should we manage that?

How do we redesign processes when we don't fully understand the algorithms that power them?

How do I know that my models and algorithms are doing the right thing?

A double-edged sword

While the digital age creates opportunities, it also creates new concerns that can undermine trust across industries and our society as a whole.

For example, constant news of data breaches, data misuse and inaccuracies is eroding public trust. What's more, technology-driven disruptions can fuel increased nationalism and protectionism as the media predicts job losses and redundancies due to automation. There also is concern that the benefits of digital transformation will not be evenly distributed, therefore worsening disparities between the haves and the have-nots.

The widespread use of AI will make it imperative — and more difficult — to ensure trusted analytics. Indeed, as organizations adopt more sophisticated analytics, machine learning models and automated decisions, many regulators are exploring new controls on all organizations that collect, analyze and use customer and business data. It's time to ask how complex algorithms will be governed to help ensure fair treatment and accurate outcomes.

And herein lies the challenge of the double-edged sword. Organizations must embrace new technology, while ensuring high, stable levels of trust in an uncertain, fast-changing digital age.

It's time to ask how complex algorithms will be governed internally to help ensure fair treatment and accurate outcomes.

The four anchors of trust

In KPMG International's 2016 report *Building trust in analytics: Breaking the cycle of mistrust in D&A*, it was proposed that trust in analytics is founded on four key anchors: quality, effectiveness, integrity and resilience. And over the past year, KPMG professionals have used this framework to help organizations assess their key trust gaps.

As noted in that 2016 report, trusted analytics is not a vague concept or theory. At its core are rigorous strategies and processes that aim to maximize trust. Some are well known but challenging, such as improving data quality. Others are relatively new and undefined in the analytics sphere, such as ethics and integrity.

So how can the four anchors improve trust in analytics?

Anchor 1: Quality

Organizations need to ensure that both inputs and analytics models are appropriate for the context in which the insights will be used. In many cases, this starts with questions about the quality of the underlying data. And as analytics become more sophisticated and machines start to do their own learning, quality also extends to the models and algorithms.

Anchor 3: Integrity

In the context of trusted analytics, integrity refers to ethical and acceptable use, from compliance with data privacy laws to less clear areas such as the ethics of profiling and predicting behaviors. This anchor is a growing concern of consumers, and it is rapidly becoming a key focus for regulators and policy-makers, as they strive to assess the 'fairness' of analytical approaches.

Anchor 2: Effectiveness

Effectiveness is about the extent to which models achieve desired results, providing value to decision makers who rely on the generated insights. When analytics are thought to be ineffective, or are used in an inappropriate context, trust can quickly erode.

Anchor 4: Resilience

Resilience is about optimizing data sources and analytics models for the long term. Cyber security is a well known example, but executives should also think about the changing use of their data sources and digital infrastructure. This kind of resilience is particularly important as analytics become self-learning and reliant on one another, using integrated algorithms to acquire input data.
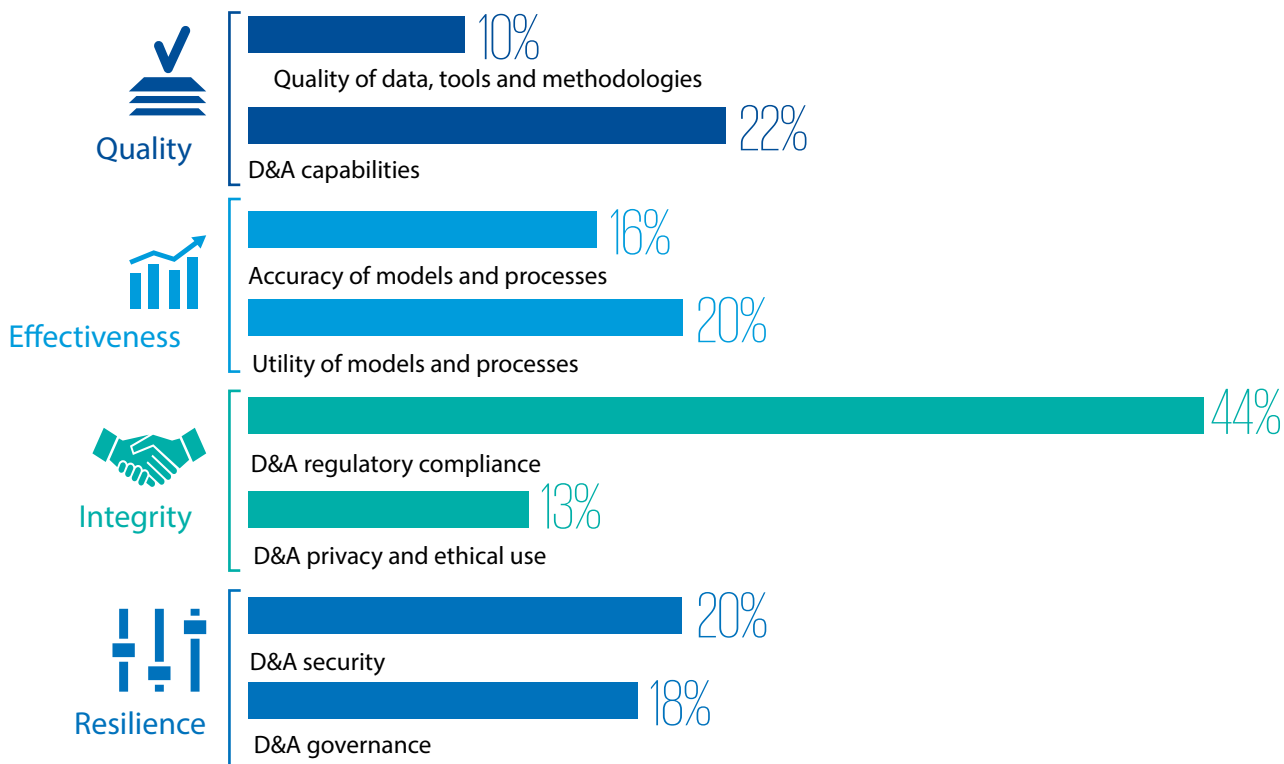
Measuring the four anchors of trust

In the 2016 survey, organizations were asked how they measured each of the trust anchors. We found that almost all organizations needed to close several capability gaps.

In fact, with the exception of regulatory compliance (where organizations tended to perform strongest),

the vast majority of respondents struggled to achieve excellence across each of the anchors. Just one in 10 respondents said they excelled in developing and managing analytics, while only 13 percent said they excelled in privacy and ethical use. Fewer than one-fifth thought they performed well in ensuring accuracy.

Figure 3
How strong are your anchors of trust? A view from 2016
How well does your organization align with best practice in each trust anchor?

Quality
- Quality of data, tools and methodologies — 10%
- D&A capabilities — 22%

Effectiveness
- Accuracy of models and processes — 16%
- Utility of models and processes — 20%

Integrity
- D&A regulatory compliance — 44%
- D&A privacy and ethical use — 13%

Resilience
- D&A security — 20%
- D&A governance — 18%

Base: 2,165 data and analytics decision makers
Source: a commissioned study conducted by Forrester Consulting on behalf of KPMG International, July 2016
Note: The chart shows the percentage of respondents who selected 'describes our approach exactly' for all of the capabilities explored under the D&A trust anchor.

The trust gap:
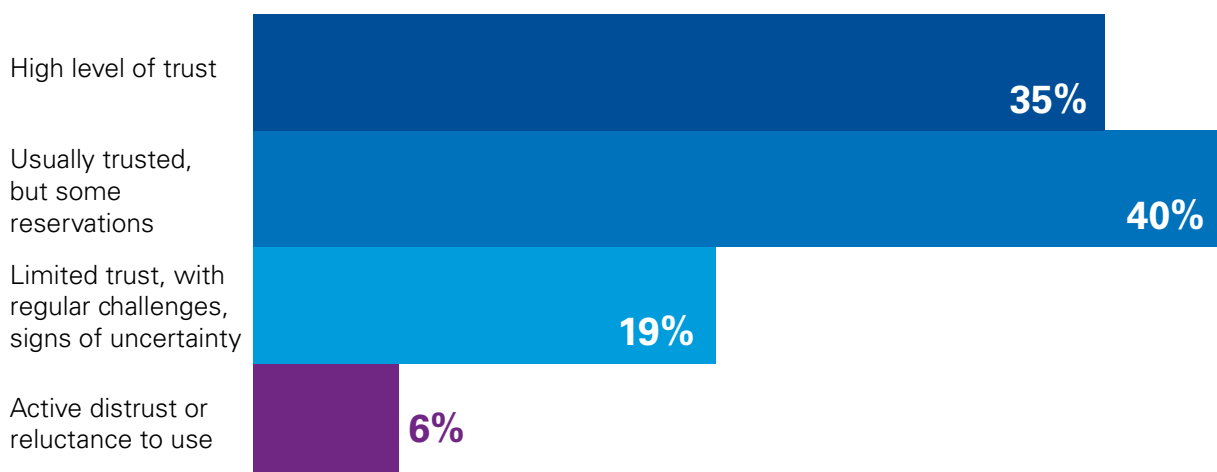# A lack of executive
confidence in analytics

Given the power that it holds, trust in D&A should be a non-negotiable business priority. Yet the *Guardians of trust* survey suggests there is a growing trust gap. Businesses want the benefits that digital and automation can deliver, but they don't always trust the underlying analytics that power those machines.

In the survey, just 35 percent of respondents said they have a high level of trust in their own organization's use of different types of analytics. A quarter admitted that they either had limited trust or active distrust.

This lack of trust does not seem to have shifted in the past year. In the 2016 KPMG *Building trust in analytics* survey, 34 percent of respondents reported a high level of trust in their operational analytics, and 38 percent professed high trust in the analytics that drive their customer insights.

Figure 4
The trust gap
To what extent do you trust the way your organization uses different types of analytics?

High level of trust	**35%**
Usually trusted, but some reservations	**40%**
Limited trust, with regular challenges, signs of uncertainty	**19%**
Active distrust or reluctance to use	**6%**

Base: 2,190 global IT and business decision makers with involvement in setting strategy for data initiatives at their organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of KPMG International, July 2017

Businesses want the benefits
that digital and automation can
deliver, but they don't always
trust the underlying analytics that
power those machines.

Reasons for mistrust

Most people already have an idea of what 'trusted data and analytics' should mean in both their professional and their personal lives. They want to know that the data and analytics are correct, and they want to know when something is wrong. They also want data to be used in a way they understand, by people they trust, and for a purpose they believe is valuable.

Some trust issues are straightforward. If management has experienced unreliable data or poor insights, they are likely to lose trust in the system they are using. But as technologies become more complex, the trust issues also become more complex.

"Executives and managers are being asked to make major decisions based on the output of an algorithm that they didn't create and don't always fully understand," noted Dr. Thomas Erwin, Head of Global Lighthouse, KPMG International. "As a decision maker, you really need to have confidence that the insights you are getting are reliable and accurate, but many of these executives can't even be sure if their models are of sufficient quality to be trusted. It's an uncomfortable situation for any decision maker to be in."

This uncertainty may increase as businesses explore more sophisticated D&A approaches. For example, AI systems may be seen as a 'black box,' making important decisions when few people outside of analytics teams, data science labs and technology centers can fully understand how.

"We often see organizations run dual processes — one managed by humans and one managed by machines — to determine whether the machine-generated insights align to those delivered by their tried-and-true, human-generated processes," says Brad Fisher, National Leader D&A, KPMG in the US. "That's simply because many executives don't have confidence that the insights are reliable and accurate."

In fact, according to the KPMG International *Disrupt and grow 2017 Global CEO Outlook* survey, more than half of respondents are concerned about their ability to integrate AI into their existing automation processes, and almost a third admitted they are not ready to adopt AI into the business.

"Many organizations are getting some comfort by testing the potential for advanced analytics and then validating the models against historical results and decisions," Professor Sander Klous, D&A Leader, KPMG in the Netherlands, says. "But when it comes to predictions based on new sources of data, some organizations don't have sufficient confidence to hand these processes over to machines."

"People will often forgive a small glitch in the data but they won't be as forgiving if the algorithms they rely on are patently wrong. It's not just about having trustworthy data, but it's also about making sure the data are being managed in a trustworthy way."

— Colin Jones, Operations Manager at Ambulance Victoria in Australia

" In 20 years' time, we may see a very different approach to pharmaceutical product approval where data is simply loaded into a machine that then decides whether a new drug will be approved or not. While you can validate a system, the system is likely to make mistakes as well. That worries me a bit because the question is whether the public will accept these mistakes as they will be different from the ones made by human beings."

— Dr. Tilo Netzer, CEO of Pharmalex
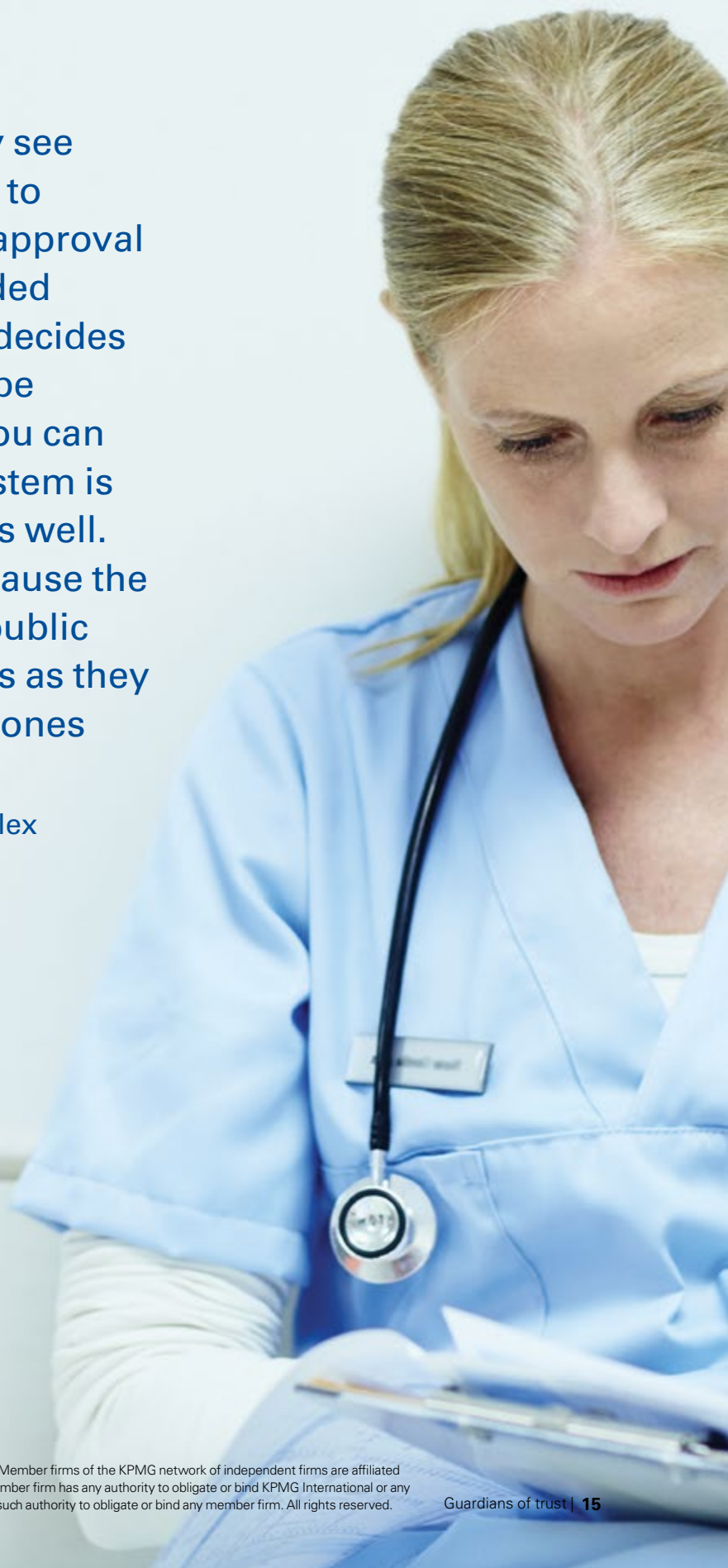
Trust goes beyond technology performance

There clearly is an opportunity for data and analytics to be proven accurate, effective and secure. But the research suggests that the trust gap has as much to do with people's expectations and perceptions as it does with the actual performance of the technology or the risks associated with it. Indeed, humans often prioritize their emotional response over their logical response, and more information does not necessarily help people build trust.

For example, the level of trust that decision makers place in their analytics seems to vary significantly by geography. The *Guardians of trust* survey shows that UK respondents are the least likely to trust their analytics, with 43 percent reporting either limited trust or active distrust. The US is close behind with 42 percent saying the same. But only 8 percent of respondents from India, 15 percent from Brazil and 19 percent from France admitted a lack of trust in their analytics. On the other hand, the survey does not show any significant variation in trust across different roles in the organization (technical or non-technical) or between the industries surveyed. This seems counterintuitive, and suggests that the variations could be due to cultural or social factors, or may relate to respondents' personal experiences with analytics and AI.

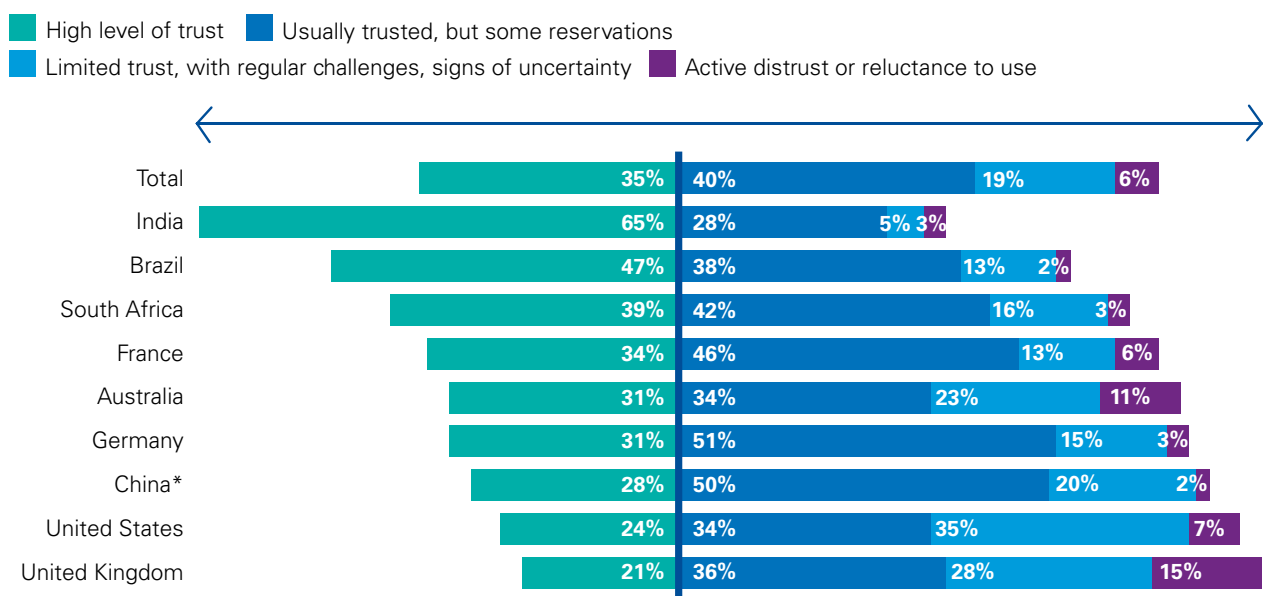"The point is that the trust gap is not the same in every country, so decision makers may need to adjust their approach depending on their market," notes Julie Caredda, Partner Data & Analytics Lead, KPMG in France. "In France, we see companies that are very keen to deploy data-driven programs to increase sales. French decision makers usually trust their analytics and they believe that data and analytics can unlock value and create new opportunities. But at the same time, these same companies are very concerned by the EU's General Data Protection Regulation. This regulation includes severe penalties of up to 4 percent of worldwide turnover in cases where companies are judged to be non-compliant." Local debate about regulation may have a negative affect on levels of trust.

In some cases, people build trust only with repeated use over many years, as we have seen with consumer technologies such as GPS, online shopping, ride-hailing services and chatbots. Education can help bridge this trust gap earlier, but the real trust comes only after a user has had repeated, successful experiences.

Finally, the ends and means are also critical for trust. For example, is the machine achieving the 'right thing' ethically, as well as financially, for all those affected by it? Is it overseen by people who exercise effective control and can manage changes, risks and uncertainties? As machines take on more day-to-day decision making, who is judging whether these controls are proper and effective?

Figure 5
The trust gap varies across countries
To what extent do you trust the way your organization uses different types of analytics?

Legend:
- High level of trust
- Usually trusted, but some reservations
- Limited trust, with regular challenges, signs of uncertainty
- Active distrust or reluctance to use

Country	High level of trust	Usually trusted, but some reservations	Limited trust, with regular challenges	Active distrust or reluctance to use
Total	35%	40%	19%	6%
India	65%	28%	5%	3%
Brazil	47%	38%	13%	2%
South Africa	39%	42%	16%	3%
France	34%	46%	13%	6%
Australia	31%	34%	23%	11%
Germany	31%	51%	15%	3%
China*	28%	50%	20%	2%
United States	24%	34%	35%	7%
United Kingdom	21%	36%	28%	15%

Note: *Inclusive of HKSAR
Base: 2,190 global IT and business decision makers with involvement in setting strategy for data initiatives at their organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of KPMG International, July 2017

Machines misbehaving: New risks

As the use of machine learning and AI increases, we may be surprised by the new ways that machines may fail us.

One likely factor in declining trust is the sobering awareness of high-profile or high-impact failures driven by algorithms, which creates new challenges for organizations, regulators and end users. In 2017, many public companies were in the headlines with crises relating to data breaches or analytics failures. In some cases, these failures were not strictly technical but resulted from an inability to predict how advanced digital technologies might perform, 'misbehave' or be perceived in the real world.

The 'superhuman' behavior problem

Many machines are of course superhuman by design. But sometimes their performance is almost 'too good' and we find ourselves unable to predict the consequences. Many believe that the first so-called 'Flash Crash'[2] of 2010 was exacerbated when hundreds of high-frequency algorithms unexpectedly reacted to a single, albeit large, futures trade. This reaction caused the major market indexes to drop by more than 9 percent (including a decline of roughly 7 percent in a 15-minute interval) before a partial rebound, resulting in the temporary disappearance of US$1 trillion in market value.[3] Today, these kinds of bot-to-bot

interactions — which can lead to high-speed 'arms races' — are also a growing risk outside the financial sector, in areas such as retail pricing optimization systems.

The 'subhuman' behavior problem

Just as algorithms can seem incredibly smart, they can also act in ways that seem surprisingly dumb. For example, people have been 'injured by GPS' when following directions that are outdated and wrong. Some cases have occurred when people drove into Death Valley and went missing due to following wrong GPS data or simply arrived in another country due to the same city names.[4]

Visual recognition is still in its infancy, despite impressive advances in some specialized areas such as medical image diagnostics. According to a recent news report, Google believes that its AI can identify and remove around 83 percent of extremist videos from YouTube, but that still leaves 17 percent that require human intervention.[5] There are also cases where researchers have 'tricked' deep-learning AI into misidentifying objects, making a computer think, for example, that a turtle is actually a rifle. This clearly is not a mistake that humans would easily make.

The 'bad-human' behavior problem

Machines can be designed to perform more fairly and ethically than humans, but algorithms that use machine learning can also pick up bad habits or biases from the human behavior they seek to emulate.[6] For instance, an algorithm used by courts to identify individuals with a high likelihood of reoffending was shown to have developed a bias against black offenders.[7] In another example, Facebook algorithms allowed advertisers to specifically target users who expressed interest in anti-Semitic subjects. Facebook has since apologized, removed bigoted categories and increased human oversight of the automated ad-buying process.[8]

There have also been cases in which algorithms have been 'taught' by malicious users to spread messages of hate and discrimination.[9] Elsewhere, some state actors have allegedly used algorithms to influence elections and sow social discord.[10] In medicine, ethical issues may increase as predictive algorithms open up avenues for treating conditions or behaviors that people have not, and may never, actually express.[11]

Who is to blame?

When an algorithm acts unexpectedly or leads to a negative outcome, who should be held responsible? While we may like to blame our machines, they are simply machines and, as such, cannot be held accountable for the decisions or insights they produce.

Should responsibility rest with the people who programmed the code? Or should it rest with the entities that sold, own or manage the machine? What about the users?

Respondents were asked which role in their organization would be held primarily responsible for a decision resulting in significant financial or customer loss due to poor analytics. Fifty-five percent said the technology function, including the chief data officer (CDO) and data scientists, would carry the brunt of the responsibility.
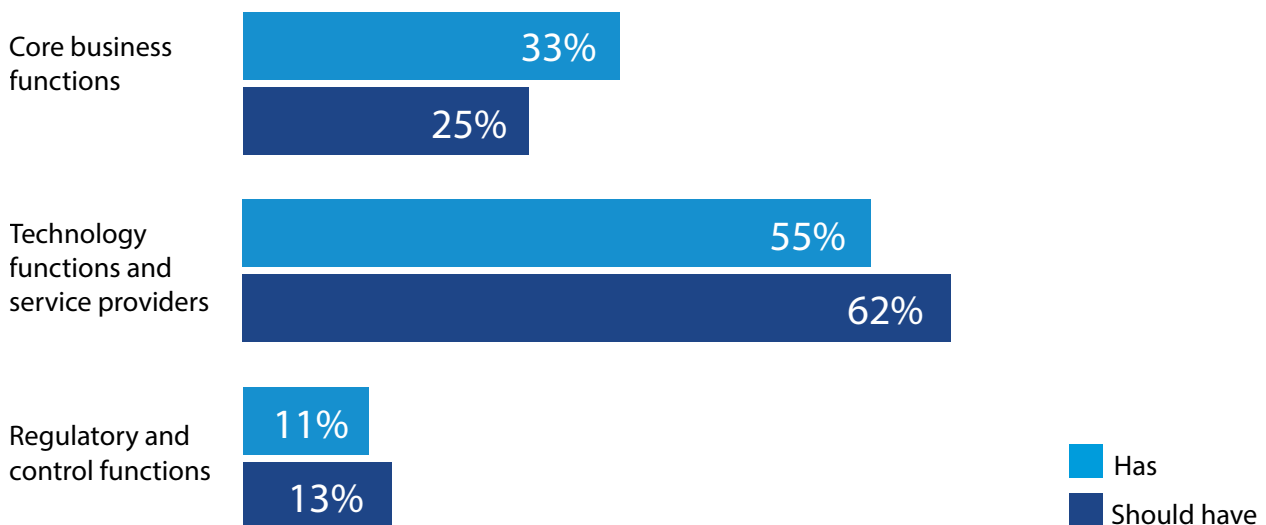
Just one in three respondents said responsibility would fall on the core business, such as the CEO and functional leaders. Furthermore, when asked who *should* hold responsibility for poor analytics-led business decisions, respondents said even more of the blame should move over from the business to technology roles.

This allocation of blame seems to mirror respondents' instincts from their lives as consumers. For example, they were asked which parties should be held primarily responsible if a fully autonomous vehicle causes an accident. The most popular response was the organization that developed the software, ahead of the manufacturer, the passenger and regulators.
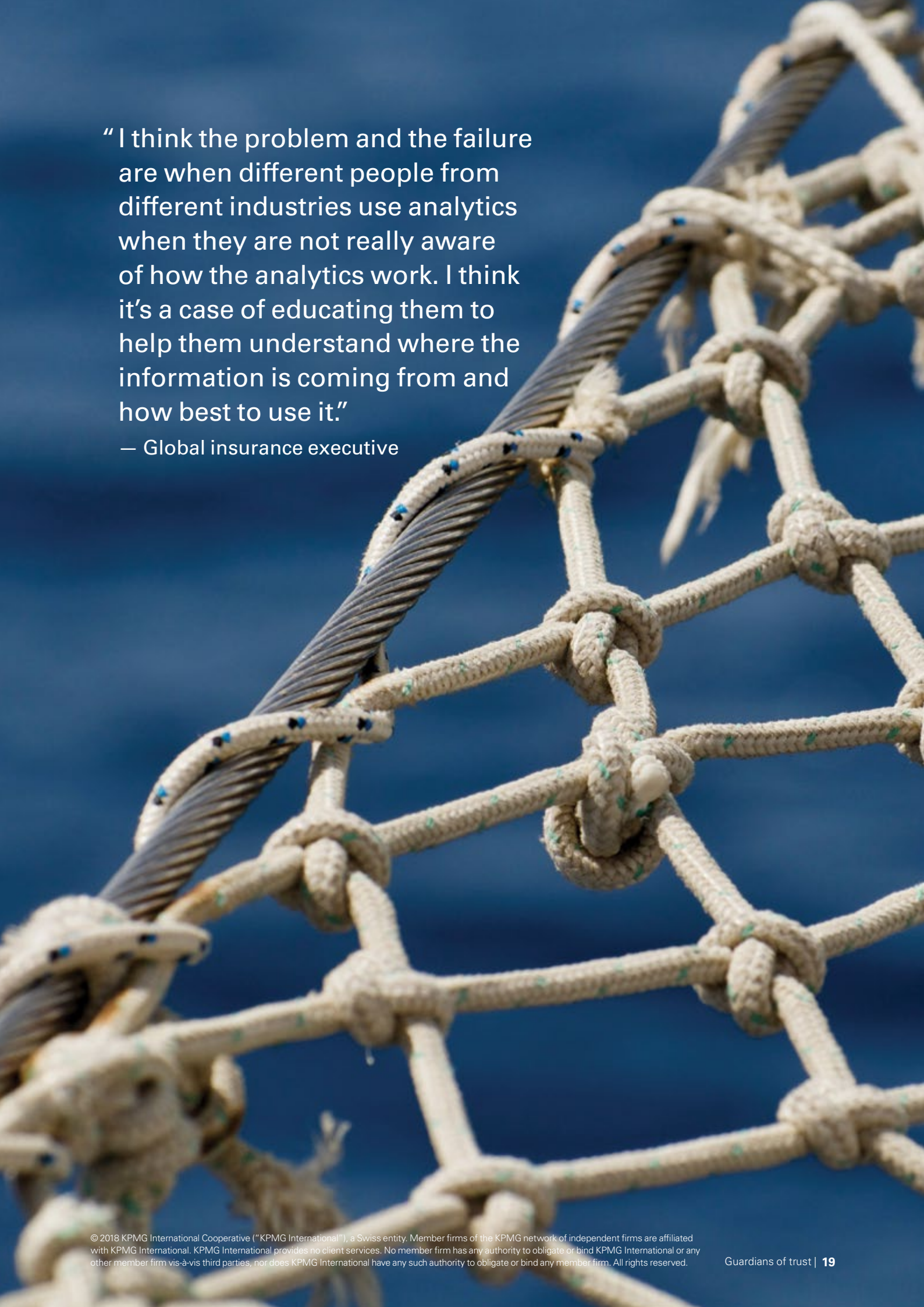
Figure 6
Where does responsibility lie?
If a poor business decision (one resulting in significant financial loss/loss of customers, etc.) is made based on insight from advanced analytics, who currently bears primary responsibility for this decision today? Who should have responsibility?

Core business functions
- Has: 33%
- Should have: 25%

Technology functions and service providers
- Has: 55%
- Should have: 62%

Regulatory and control functions
- Has: 11%
- Should have: 13%

Legend:
- Has
- Should have

Base: 2,190 global IT and business decision makers with involvement in setting strategy for data initiatives at their organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of KPMG International, July 2017
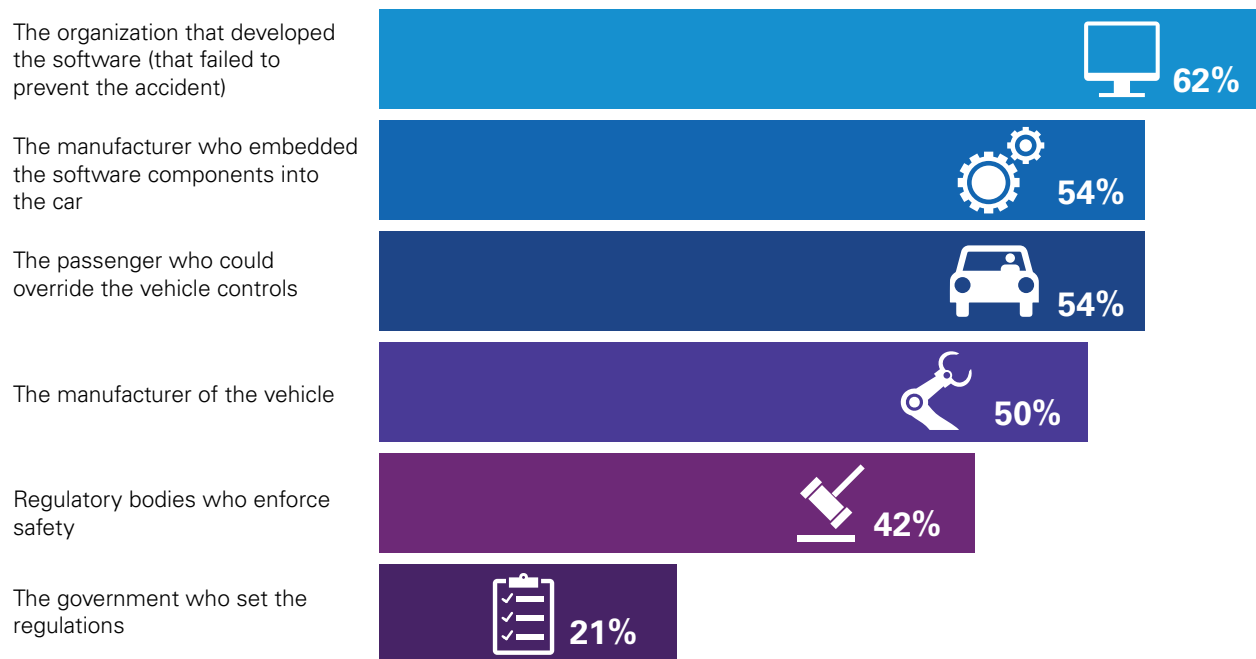
" I think the problem and the failure are when different people from different industries use analytics when they are not really aware of how the analytics work. I think it's a case of educating them to help them understand where the information is coming from and how best to use it."

— Global insurance executive

Figure 7
Spreading the blame
If a non-fatal accident was caused by an autonomous vehicle while the human driver was not in control, who do you believe should be primarily responsible for the accident? (Select all that apply.)

The organization that developed the software (that failed to prevent the accident)	62%
The manufacturer who embedded the software components into the car	54%
The passenger who could override the vehicle controls	54%
The manufacturer of the vehicle	50%
Regulatory bodies who enforce safety	42%
The government who set the regulations	21%

Base: 2,190 global IT and business decision makers with involvement in setting strategy for data initiatives at their organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of KPMG International, July 2017

In both scenarios (corporate analytics and autonomous vehicles), the responses also suggest that risk and regulatory functions should shoulder a certain level of responsibility. Inside the organization, 13 percent of respondents suggested the blame should rest primarily with internal risk and audit functions — or with external risk functions such as regulators and third-party auditors. From a consumer perspective, 42 percent of respondents said blame for an autonomous vehicle accident should rest with regulatory bodies.

"It's too easy for people to think 'It's black and white. It's science, and you told me this is the answer', when in fact it is not so straightforward at all," says Brad Fisher, National Leader D&A, KPMG in the US. "The next step is to think about different levels and types of responsibility.

The C-suite is going to have one level of responsibility. The business leader below them who maybe is making the decision has a different level, and the technical people have a different level of responsibility. But it's hard to make this work well on the ground."

Herein lies a key challenge: According to the research, leaders' impulse is to absolve the core business for decisions made with machines. This impulse is understandable given technology's legacy as a support service, the difficulty of assessing the trustworthiness of analytics, and the tendency to give all things technical 'to the experts'. However, many IT professionals simply do not have the domain knowledge — nor the overall capacity — required to ensure trust in D&A. Instead, as we explore in the coming pages, the responsibility should rest with the core business.

Leaders' impulse is to absolve the core business for decisions made with machines.

" It's too easy for people to think 'It's black and white. It's science, and you told me this is the answer', when in fact it is not so straightforward at all. The next step is to think about different levels and types of responsibility. The C-suite is going to have one level of responsibility. The business leader below them who maybe is making the decision has a different level, and the technical people have a different level of responsibility. But it's hard to make this work well on the ground."
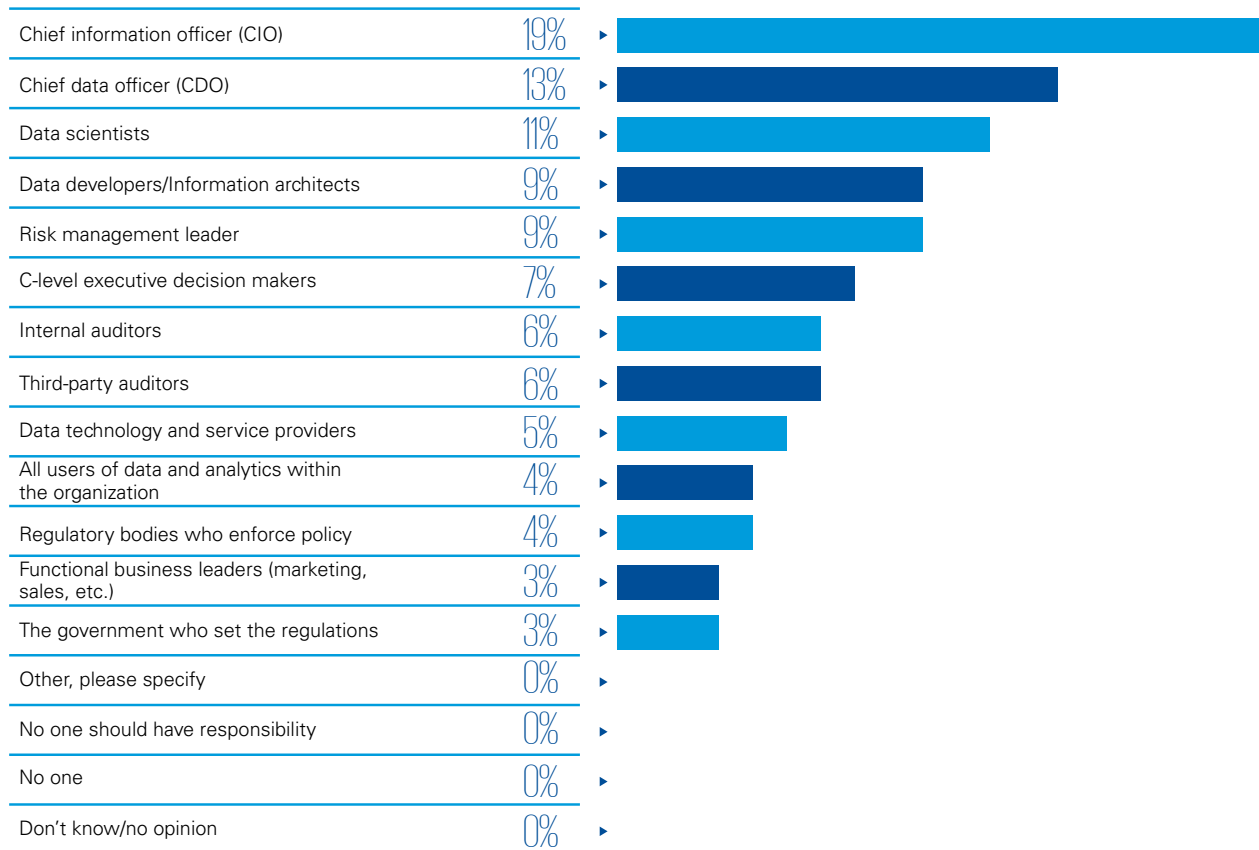
— Brad Fisher, National Leader D&A, KPMG in the US

Governance: Taking responsibility for trusted analytics

While it is easy to point fingers when things go wrong, the harder task is to proactively govern analytics in ways that build trust, resilience, integrity, quality and effectiveness. While there is a growing sense that organizations should be more accountable for their use of D&A, best practice in governance is yet to be defined.

Figure 8
Uncertainty about governance
Who in your organization has primary responsibility for ensuring the trustworthiness/accuracy of advanced analytics and models?

Chief information officer (CIO)	19%
Chief data officer (CDO)	13%
Data scientists	11%
Data developers/Information architects	9%
Risk management leader	9%
C-level executive decision makers	7%
Internal auditors	6%
Third-party auditors	6%
Data technology and service providers	5%
All users of data and analytics within the organization	4%
Regulatory bodies who enforce policy	4%
Functional business leaders (marketing, sales, etc.)	3%
The government who set the regulations	3%
Other, please specify	0%
No one should have responsibility	0%
No one	0%
Don't know/no opinion	0%

Base: 2,190 global IT and business decision makers with involvement in setting strategy for data initiatives at their organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of KPMG International, July 2017

Who has primary responsibility for governing the trustworthiness and accuracy of advanced analytics? The survey suggests significant uncertainty. The CIO received the most votes (although only 19 percent), and respondents also nominated a wide range of other roles. Twelve percent named the CDO, 13 percent named data scientists and 9 percent named data developers.

Somewhat surprisingly, 18 percent of respondents suggested that primary responsibility for ensuring trustworthiness should sit with roles outside the organization altogether — with external suppliers, third-party auditors, regulators or government.

" The CEO is ultimately held responsible but that means companies need to have a system in place to ensure that things have been developed appropriately and that the proper quality checks are in place. If everything has been done according to expectations, there may be nobody to blame. There is always a risk when working with new technologies."

— Dr. Tilo Netzer, CEO of Pharmalex

Who is holding the anchors in place?

To better grasp the governance challenge, respondents were asked who should hold responsibility for D&A across the four trust anchors (identified on page 10). Across the board, respondents maintained that the primary responsibility should rest within the technology function.

Only 27 percent said the business should take responsibility for effectiveness, ensuring that the outputs of models work as intended and deliver value to the organization in practice. For integrity and resilience, including ethics, even fewer respondents assigned responsibility to the business. For resilience, more than a quarter gave primary responsibility to risk management leaders, internal auditors, third-party auditors and regulatory authorities.
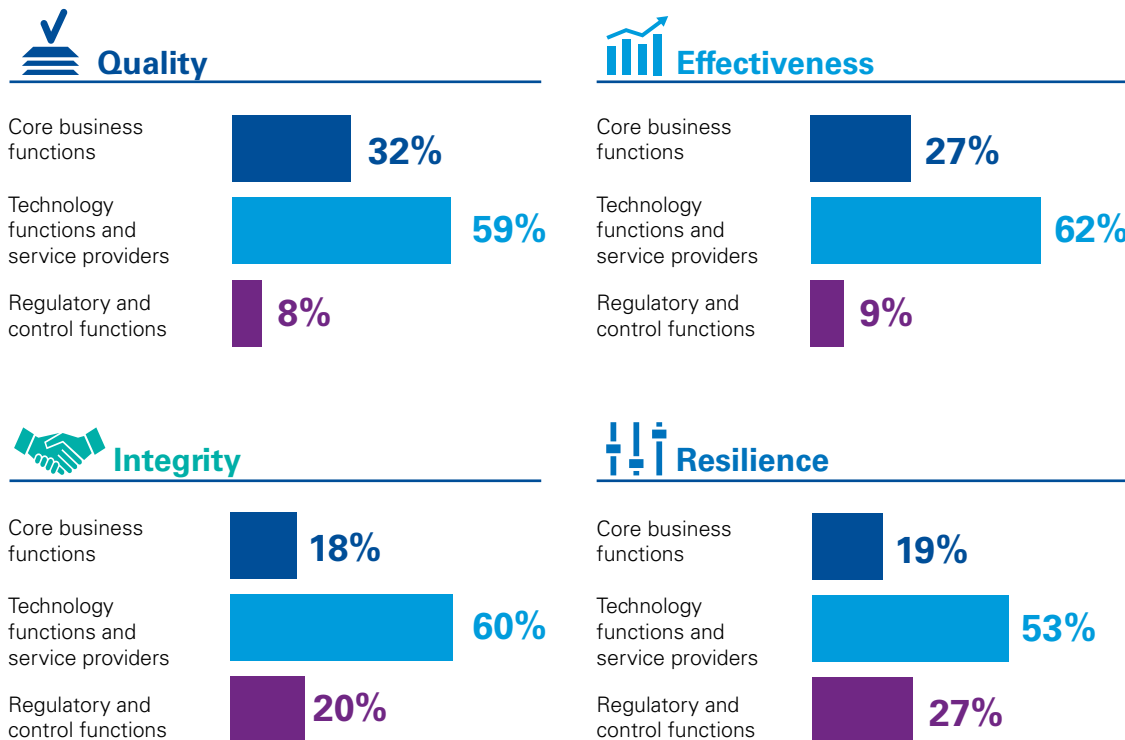
Misplaced accountability

These results are troublesome for the future. They again suggest that, at best, there is a lack of clarity around the core business' ownership of the impact of analytics. At worst, the core business is absolved of responsibility altogether.

The purpose of risk functions and regulators is not to be responsible for core business systems but rather to ensure effective controls and processes. Moreover, blaming regulators for failing to anticipate misuse or bad outcomes provides no shelter from potential reputational damage.

External providers, meanwhile, do play critical roles in digital transformation but that does give businesses an excuse for avoiding responsibility.
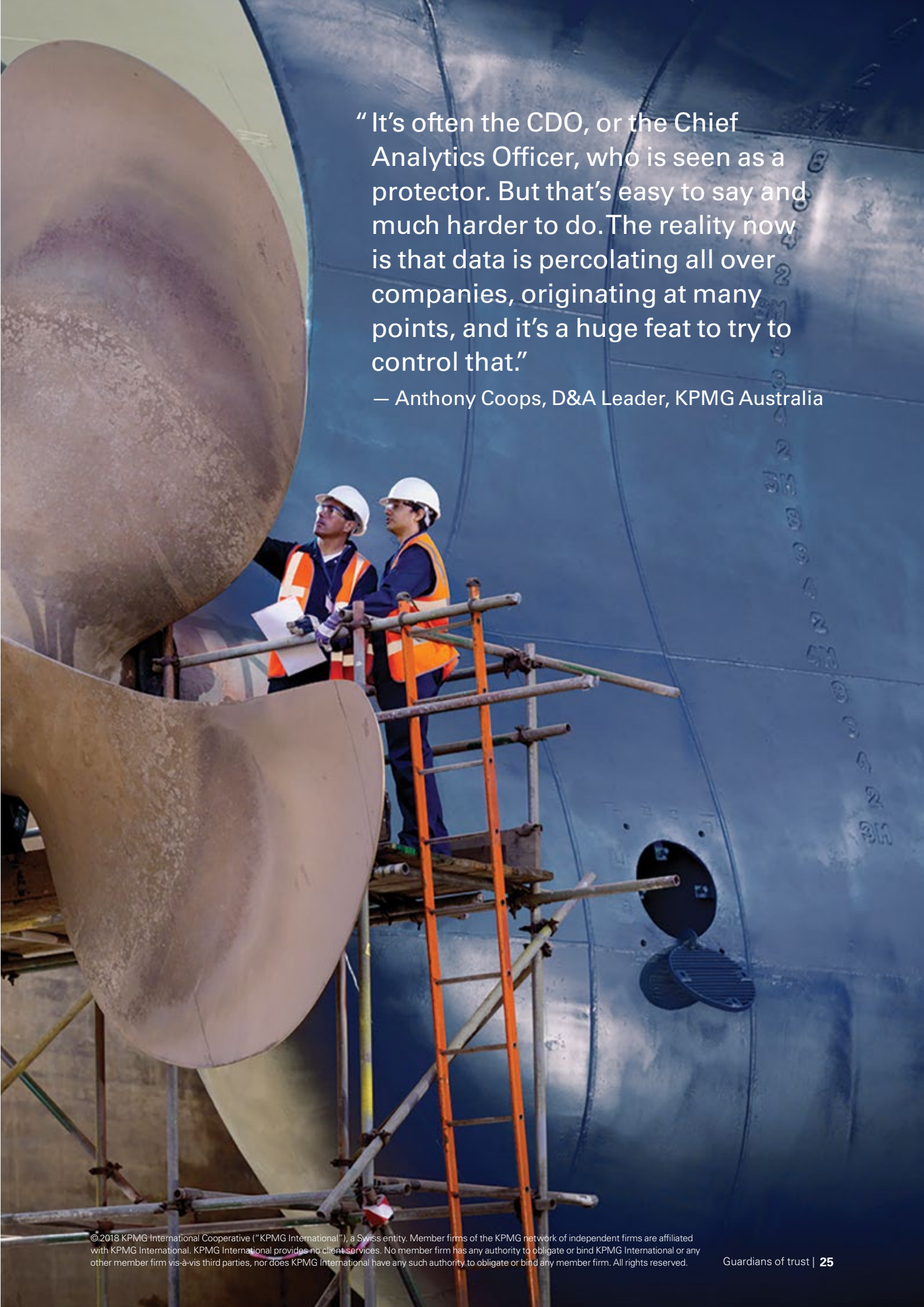
Figure 9
Different hands on different anchors
Who in your organization should have primary responsibility for the following areas of data and analytics?

Quality
Core business functions	32%
Technology functions and service providers	59%
Regulatory and control functions	8%

Effectiveness
Core business functions	27%
Technology functions and service providers	62%
Regulatory and control functions	9%

Integrity
Core business functions	18%
Technology functions and service providers	60%
Regulatory and control functions	20%

Resilience
Core business functions	19%
Technology functions and service providers	53%
Regulatory and control functions	27%

Base: 2,190 global IT and business decision makers with involvement in setting strategy for data initiatives at their organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of KPMG International, July 2017

" It's often the CDO, or the Chief Analytics Officer, who is seen as a protector. But that's easy to say and much harder to do. The reality now is that data is percolating all over companies, originating at many points, and it's a huge feat to try to control that."

— Anthony Coops, D&A Leader, KPMG Australia

As for the technology function, most respondents in the survey expect technical people to ensure the trustworthiness of analytics and take on wider responsibilities. This function includes what we will call the 'data suite' (D-suite) and the 'analytics suite' (A-suite) — in other words, the CDO, data scientists, data developers and IT managers. But both the D-suite and the A-suite are under increasing pressure from the business to manage multiple emerging objectives.

"It's often the CDO, or the Chief Analytics Officer, who is seen as a protector," says Anthony Coops, D&A Leader, KPMG Australia. "But that's easy to say and much harder to do. The reality now is that data is percolating all over companies, originating at many points, and it's a huge feat to try to control that".

For example, conversations with CDOs suggest they are expected not only to ensure the quality and integrity of data, but also to create and manage external relationships, create opportunities for data monetization, improve the reliability of internal reporting and forecast

the organization's analytics needs. Few seem to have the resources or the inclination to take on greater responsibility for the overall governance of AI and analytics across the core business.

"The responsibly often falls on me as the lead data architect," says a director at a European financial services organization. "But I think the executives I provide the reports to are also responsible. They need to use this as part of their judgment — they need to take ownership".

Traditional frameworks for IT governance have been seen as subsets of corporate governance. In practice they have focused on managing performance and rely heavily on processes operated by the IT function. Ultimately, there are huge areas of risk and responsibility that may not be effectively managed by traditional governance models. For organizations undergoing rapid digital transformation there is a clear need to find new ways of working that balance the desire for expert technical oversight with the reality that the core business is increasingly digital.

"The responsibility often falls on me as the lead data architect. But I think the executives I provide the reports to are also responsible. They need to use this as part of their judgment — they need to take ownership".

— director, European financial services organization

Microsoft: Designing a principles-based approach

An interview with **Emma Williams, General Manager for Microsoft's Bing.com** search engine user experience and a recognized leader in the field of AI ethics.

What is your vision for AI?

At Microsoft, our mission has always been to empower every person and every organization to achieve more. And we see AI as a fundamental way to amplify human ingenuity. Right now, our focus is on trying to blend what we call EQ, or 'emotional intelligence,' with traditional IQ, so we can create computers that can truly understand us in a much warmer and more empathetic way.

How are you addressing the ethical implications of AI from a strategic perspective?

We are thinking about a broader context that includes fairness, accountability, transparency and ethics: an approach we call AI FATE. Ethics is one part of the equation, which is really all about making sure humans remain at the center. But we are also thinking about how we ensure fairness and remove bias. We're thinking about how we make the training of AI more accountable. And we're talking about how we help people understand the mechanism behind the AI and the impact it has on their lives and activities.

In such a rapidly evolving field, how do you ensure you remain at the forefront of these issues?

The reality is that we are inventing the future as we go along and there are no existing design templates or user experience patterns to model. My team includes the classic UX designers that you would expect to see, but we also have people with PhDs in human psychology and cognitive behavior, as well as ethicists, anthropologists and psychologists.

How do ethical and trust considerations influence the product development and user experience strategy at Microsoft?

We're very committed to a principles-based approach when designing our products and user experiences. And for the past year, we've been working on developing a set of AI design principles that will be embedded into our products. Some are core to our vision of putting the human at the center and understanding the context within which the AI will be used. Others are more focused on creating a warmer experience — integrating that EQ aspect — when interacting with the AI.

Who should be responsible for creating trust standards and expectations for AI?

I'm not sure any one party is responsible. That is why, last year, we founded the Partnership on AI along with IBM, Google, Amazon and others. Today, the Partnership includes more than 40 of the top tech companies and about 30 nonprofit organizations. As the Partnership defines and debates the ethical nuances, I believe we will start to see standards emerge that will hold for the broader industry.

What advice would you offer executives as they look to the future?

I think the best advice is to really think deeply about who you are building AI for and what they want to achieve. It's really going back to first principles about knowing your customer and focusing the business on the value that you give them. If you continue to do that and really focus on making the human the hero, it starts to become easier to wrap your head around some of the ethical implications and decisions that need to be made.

Building the governance of AI into the core business

KPMG professionals believe that as advanced analytics become integral to business operations, the management of machines is as important as the management of people. Therefore, the governance of machines must become a core part of the governance of the whole organization. The goal should be to match the potential power and risk of data and analytics with the wisdom to optimize value, in the context of each organization and the society in which it sits.

The experience of early adopters suggests that AI is not fundamentally about technology outputs, nor is it about replacing people to reduce costs. Rather, it is about a blended human and digital workforce that shares decisions as well as tasks.

As organizations think about the behavior of machines as parallel to the behavior of people, they also are considering new models of governance to support the leaps in trust that this new workforce requires. At a fundamental level, ownership of machines must be held firmly by the CEO and functional leaders.

Human oversight by a range of different domain experts is a critical part of governing advanced analytics. For example, systems at risk of high-impact 'misbehavior' require constant attention, which will be especially critical in contexts such as driving on busy roads or interacting with customers and the public. In addition to technical and industry expertise, these kinds of scenarios require participation from ethicists, anthropologists, psychologists, lawyers and 'ordinary' members of the public. This oversight will help build trust in AI and optimize performance at the boundary between human and machine.

" The governance of machines must become a core part of governance for the whole organization."

— Nadia Zahawi, Director, D&A, KPMG in the UK

Governance: Changing frameworks of enablers and controls

The 'guardians of trust' are of course not just people with new responsibilities. We are also seeing the expansion of standards and controls from the purely technical into softer strategic, cultural and ethical domains. These standards and controls are also expanding from early stages of the software lifecycle to a whole-life, whole-system view.

While there are many technical standards to support the development of IT systems and tools, these standards need to be aligned, improved and adapted. There are recognized gaps and inconsistencies in areas of emerging risks such as AI testing, data privacy and ethical standards.

Figure 10
Top five recommendations for building public and customer trust in data and analytics (as suggested by respondents)

1. Develop standards to provide guardrails for all organizations.

2. Modernize regulations to build confidence in D&A.

3. Increase transparency of algorithms and methodologies.

4. Create professional codes for data scientists.

5. Strengthen internal and external assurance mechanisms.

For example, under the European Union's new General Data Protection Regulation (GDPR), organizations that carry out large-scale monitoring of individuals must appoint a data protection officer (DPO). However, where DPOs do exist, their mandated role is often limited, focusing on legal compliance with the GDPR.

There are particular governance challenges where multiple parties are involved. Shared data and analytics platforms are becoming more common, for example in healthcare, scientific research and 'smart city' initiatives. "We see clients asking for help with the management of platforms that involve multiple competitors and other players in a value chain, which is not overseen by any clear guardian of trust, unlike Uber or Facebook," says Professor Sander Klous, D&A Leader, KPMG in the Netherlands. "They need to create a very broad ecosystem that delivers a range of services and adds value. We expect to see new frameworks put forward by regulators or other authorities with certain rules and regulations, and obligations to hire an independent third party to ensure that they comply with these rules and regulations. This role may become a type of data and analytics accountant".

In some cases, existing governance frameworks could be adjusted to fit the analytical enterprise of the future. For example, a common and widely accepted governance principle is the 'three lines of defense' framework, which helps organizations clearly identify roles and responsibilities in the business and practice ongoing risk management.

1. The business. As the first line of defense, the business units must be aware of the analytics they are using and be able to manage the four anchors of trust: the quality, effectiveness, integrity and resilience of their algorithms.

2. Risk oversight. As the second line of defense, the risk-oversight functions will need to establish policies and procedures that serve as guardrails for the organization.

> " We see clients asking for help with the management of platforms that involve multiple competitors and other players in a value chain, which is not overseen by any clear guardian of trust, unlike Uber or Facebook."
>
> — Professor Sander Klous, D&A Leader, KPMG in the Netherlands

3. Assurance and audit. As the third line of defense, independent assurance providers and internal auditors should validate the controls and identify potential areas of weakness.

Interestingly, in analytical organizations, these three lines of defense are starting to evolve. In banking and high tech sectors, for example, some of the policies and procedure checks created by the second line of defense may now be automated within the processes of the first line of defense, for example by bots that check compliance or flag risks. Meanwhile, internal auditors as part of the third line of defense may now include data scientists who traditionally only sat in operational roles within the first line of defense.

A growing number of organizations recognize that audit evidence and business insight are two sides of the same data. And by enabling auditors to analyze unstructured data, AI can help decision makers to obtain evidence and insights that allow them to make more confident decisions and conclusions about the areas of audit focus. In the future, AI can increasingly allow auditors to obtain and analyze information from non-traditional sources, such as all forms of media — print, digital and social — and, combined with other information, draw a deeper, more robust understanding of potential business risks. Predictive analytics capabilities will likely be developed further, enabling auditors to take information from multiple sources and apply it to the outlook and risks facing businesses.

As such, organizations also need to look beyond the human oversight of machines in core operations. Organizations also need to ensure trust in the human-machine partnerships, which increasingly underpin corporate governance and ensure public trust in business as a whole.

KPMG Clara

KPMG Clara client collaboration is an online tool that facilitates secure collaboration between KPMG and clients. It is used by both group and component teams and promotes seamless communication, giving continuous visibility into key audit tasks in real time.

Through advanced tracking and monitoring capabilities, KPMG teams can access the information they need when they need it, whether that is the latest updates on audit discussion topics/issues, the status of the prepared by client (PBC) process or the progress of group reporting by component auditors.

" KPMG Clara client collaboration is also the way we will deliver outputs from the data and analytics capabilities, which provide greater transparency to the audit and access to deeper insights, which can ultimately enhance trust and confidence in financial reporting." — Murray Raisbeck, D&A Leader, KPMG in the UK

Amsterdam ArenA: Building an ecosystem of trust

An interview with **Henk van Raan, Chief Innovation Officer and Director of Facility Management for Amsterdam ArenA,** one of Europe's leading stadiums and concert venues.

What is Amsterdam ArenA's vision for data and analytics?

Data and analytics have allowed us to develop a much richer understanding of how we can better serve our visitors, but also keep them safe - how we can optimize their experience and the way they move around and inside the stadium. We use data from cameras, ticket sales and traffic systems to help steer the crowds and avoid congestion around the stadium. Yet this is just the beginning. In the next phase, we hope to leverage more sophisticated AI technologies to help automate some of those decisions on a real-time basis and, ultimately, become a testing ground for future `smart city' applications for the city of Amsterdam.

How are analytics approaches developed and implemented within the arena?

The core Amsterdam ArenA team is very small, which is why we focus on partnerships to recruit and develop certain capabilities around data, analytics, innovation, business modeling and so on. We see ourselves as an `innovation arena' or digital playground for innovators — small entrepreneurs and big enterprises — who are looking for opportunities to combine our data and their knowledge to create new services and a safer city.

Are you concerned about the quality of the data or analytics that are being shared by your partners?

We recognize that, for innovation to thrive, all parties must have a high level of trust in the data environment. This is why we developed a robust data governance process that complies with Dutch regulatory laws. Analytics and data availability are always linked to a clear goal, which provides a framework for both quality assessment and control. In the future we expect to be able to manage those processes better by leveraging blockchain or other distributed ledger systems.

How are you developing public trust in the way you collect and use customer data?

I think everyone starts out being cautious about how their information is being used. If you can make a very solid case for value — clearly demonstrating the benefits for consumers — it becomes much easier to build public trust. We also have a rigorous process in place to ensure that our partners abide by the rules and regulations when dealing with personal information. I think that the key to trust is clear communication and transparency about your actions. Our customers understand that we use data to improve security, safety and enjoyment, so they are usually happy to be involved.

Do you see a need for regulation or standards around the use of data and analytics?

I suspect we will see more rigor around the assessment of data and analytics models, possibly including a form of audit or alignment to global standards. For now, I think the focus for companies and innovators is to be as transparent as possible with their customers about how their data is being used, along with the potential benefits or risks. In parallel, data analysts should also actively keep asking themselves "why are we doing this?" and "is this still in line with our common goal?"

Eight areas of essential controls for trusted data and analytics

For an analytical enterprise, an effective framework of enablers and controls is a board priority. KPMG professionals are seeing a range of new roles and ways of working across the organization to strengthen the four anchors of trust, effectively creating a distributed system of trust for the digital age. These eight areas may form the basis of a more strategic, integrated and distributed framework for governance of trusted analytics.

"Building trust requires customized actions," says Dr. Thomas Erwin. "One size doesn't fit all. People realize there needs to be controls around data and analytics. But there's a line to walk between agility and control. That's the trade-off where a lot of people are struggling. It's important to make your own assessment against the four anchors of trust. We are seeing a lot of experimentation with new enablers and controls that are likely to drive future standards and new governance frameworks."

A wide range of ideas are emerging across eight essential enabling areas as the basis for ensuring trusted analytics:

1) Structure and roles	Example
Many organizations are evolving from a centralized, IT-driven model — or from a 'wild west' model of multiple teams — toward a more organized, scalable, distributed approach. Many clients are creating powerful centers of excellence which, in addition to providing technical expertise, also oversee a system of trust, including risk management, innovation, standards, support and education. This may be part of a governance model at multiple scales: data ownership, algorithm ownership, portfolio ownership and ecosystem ownership.	**Partnering and 'parenting' algorithms** Banks are beginning to identify a nominated human partner in the core business, responsible for each critical algorithm. The concept of 'parenting' AI throughout its lifecycle is also gaining traction. 'Parenting' recognizes that machines can be considered as demonstrating behaviors that change over time and in different contexts, and it will not be enough to teach or test AI in a narrow technical context.
2) Regulation and standards	Example
Beyond compliance with current legal and regulatory requirements, organizations are also considering proactive moves in areas of standards and 'regulatory lag' (where there is a gap between what society expects and what is considered a minimum legal requirement). This gap often creates trust issues and can lead to post-hoc exposure to large fines or reputation damage. The gap may need to be fixed manually. For example, some social media sites are greatly increasing the number of human content moderators.	**'Explainable AI'** Even if it can be technically explained (which is not always the case), AI's decision making process is usually too difficult for most people to understand, including regulators. The purpose of 'explainable AI' is to ensure machine-learning systems have the ability to explain their rationale to humans and provide some understanding of how they will behave in future. This is particularly critical for high risk AI, for autonomous vehicles and robots in defense, for example.

3) People and culture	Example
Many clients are particularly active in this area, including initiatives in communication, education, training, job design and user experience design — within and beyond the walls of the organization.	**Human-machine job evaluations** A telco organization is changing its job evaluation policies to take into account a mixed workforce of bots and humans. Traditional job evaluation assumed a lower job grading for jobs with greater automation or decision support, but the telco recognized that these staff were responsible for increased output and higher-value functions. The company changed its job evaluation approach to account for human-machine workforces.

4) Strategic alignment	Example
It is increasingly critical to ensure that the use of machines aligns with cultural and social values as well as internal business strategy and objectives. Concepts of fairness, for example, vary significantly between geographies and may need new mechanisms to ensure ongoing oversight and debate.	**Ethics boards** Silicon Valley giants Google, DeepMind, Facebook, Amazon, IBM, Apple and Microsoft joined forces to create the Partnership on Artificial Intelligence to Benefit People and Society.[12] This organization aims to advance public understanding of the sector, as well as develop standards for future researchers, which align with perceived cultural and social values.

5) Processes	Example
Beyond standard IT development and quality assurance processes, organizations are creating new processes to improve the design, performance and auditability of algorithms. Design thinking and customer journey mapping are becoming standard capabilities to bring bot-building out of the sole control of the technology function.	**Human-centered machine learning** Before developing an algorithm, Google focuses on how people might solve a problem manually.[13] This approach connects the development team to the users and highlights the outputs that have the largest impact.

6) Data management	Example
The explosion of data sources and uses is driving a wide range of new approaches to data management. The collection and use of data is generally shifting from a central IT function to a wide range of partners and stakeholders within an ecosystem that needs more careful management and controls.	**Independently curated data** Amid the growing number of data sources, organizations are using independently 'curated' data[14] — verified by a trusted source — before using it under agreed conditions. Some companies are creating data depositories, enabling individuals or organizations to define and control the use of their data, and put a wall between the data they are willing to share and the data they are not.

7) Technology	Example
As a control mechanism, organizations are increasingly using machines to oversee other machines, while ensuring that humans can intervene if needed. This approach can include built-in master off switches, intentionally reduced complexity, 'go-slow' modes on processing speed, and real-time 'watchdogs' of algorithm behavior.	**RegTech** High-speed algorithmic financial trading relies on code to examine and regulate the vast volumes of trades, which cannot be encompassed by humans.

8) Alliances and ecosystems	Example
As organizations create common platforms for improved analytics, they need new trust frameworks to ensure all parties are managing data properly. Organizations can also achieve great value by partnering with others to create governance ecosystems.	**Blockchain** As Henk van Raan notes in his interview on page 31, Amsterdam ArenA is building common processes to ensure that partners abide by certain rules and procedures for the use of data within the Amsterdam community. The organization expects to leverage blockchain or other distributed ledger systems to support the alliance.

In summary

In the digital age, trusted analytics will be a critical source of competitive advantage. And the road to trust is paved with a thoughtful, strategic approach to governance — one that stretches well beyond the traditional focus on technology and risk. Indeed, amid the unprecedented use of D&A to drive decisions and the growing human-machine workforce, the governance of machines must become more strategic and integrated with governance of the entire enterprise.

Gone are the days when IT can be the catchall for anything related to technology. Instead, it's time for the core business to take responsibility for its analytics and AI — and ensure quality, effectiveness, integrity and resilience.

To that end, chief executives and functional leaders will need to manage machines as rigorously as they manage their people. Such an approach requires standards and controls that go beyond the operational to also focus on the cultural, ethical and other emerging considerations for managing advanced technology across the enterprise.

1 **If you can't measure it, you can't manage it**
Start by assessing the level of trust that users place in existing analytics and the related controls. The Four Anchors of Trust are a useful framework for this exercise.

2 **Prioritize risks**
Don't try to do everything at once. As the trust framework is being developed, focus on those that pose the greatest risk for the organization and its stakeholders.

3 **Create trust-impact personas**
Ensure that your organization is thinking about all of the stakeholders impacted — managers, customers, regulators, markets and media, for example.

4 **Create a buddy system**
Make sure all business-critical and high-risk algorithms have a human partner who is accountable for their performance and impact.

5 Stay legal
Track the changing landscape of regulations and create alignment between not only current regulations and requirements, but also those that can be predicted to arise in the future.

6 Create a manifesto for data and analytics
Provide employees and process owners with appropriate guidelines, particularly in fast-changing areas such as ethics, transparency, accountability and auditability.

7 Don't let the board off the hook
Ultimately, executives and boards will remain responsible for the actions and inactions of an organization. Educate them in technology risks and controls.

8 Be flexible with horses for courses
Don't focus on just one standard approach or framework to define and improve your controls.

9 Review your governance framework
No one party can be wholly responsible for algorithms, which means that governance and controls must also be distributed among multiple internal and external parties.

10 Point fingers carefully
Create clear responsibilities and accountabilities for specific systems or algorithms to spot potential challenges that may occur over time and prevent unexpected errors.

Methodology

Survey demographics: Country and employees

In which country do you work?
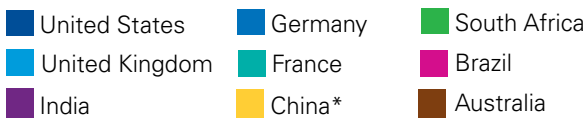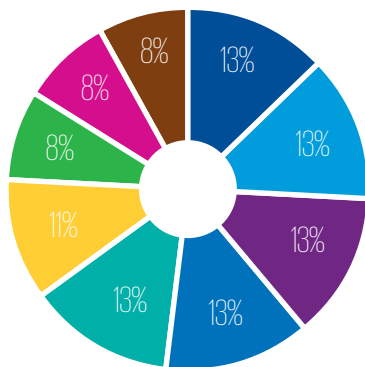
■ United States	■ Germany	■ South Africa
■ United Kingdom	■ France	■ Brazil
■ India	■ China*	■ Australia

Note: *Inclusive of HKSAR
Base: 2,190 global IT and business decision makers with involvement in setting strategy for data initiatives at their organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of KPMG International, July 2017

Using your best estimate, how many employees work for your firm/organization worldwide?
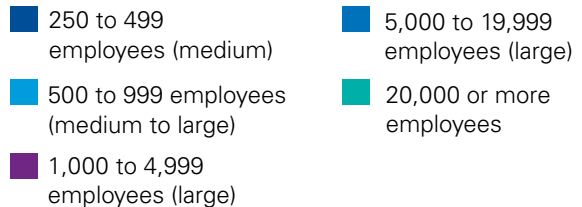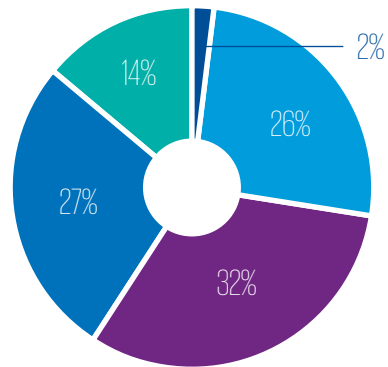
■ 250 to 499 employees (medium)	■ 5,000 to 19,999 employees (large)
■ 500 to 999 employees (medium to large)	■ 20,000 or more employees
■ 1,000 to 4,999 employees (large)	

Note: percentages do not total 100 percent due to rounding.
Base: 2,190 global IT and business decision makers with involvement in setting strategy for data initiatives at their organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of KPMG International, July 2017

> Leaders from KPMG International, KPMG member firms, clients and alliance partners also contributed analysis and commentary to this study.

Note: percentages do not total 100 percent due to rounding.

Survey demographics: Industry and title

Which of the following best describes the industry to which your company belongs?
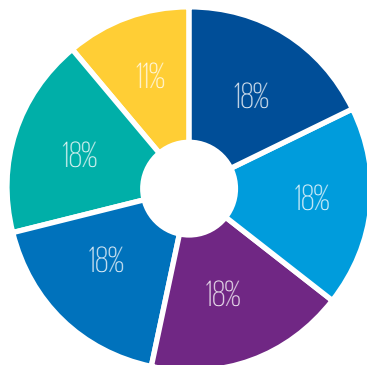
- ■ Telecommunications services
- ■ Retail
- ■ Insurance
- ■ Healthcare/life sciences
- ■ Financial services/ Banking
- ■ Retail

18% 18% 18% 18% 18% 11%

Note: percentages do not total 100 percent due to rounding.
Base: 2,190 global IT and business decision makers with involvement in setting strategy for data initiatives at their organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of KPMG International, July 2017

Which title best describes your position at your organization?
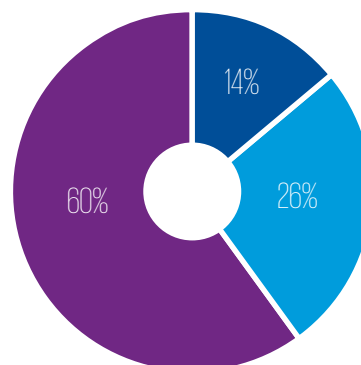
- ■ C-level executive (e.g., CEO, CMO)
- ■ Vice president (in charge of one/several large departments)
- ■ Director (manage a team of managers and high-level contributors)

14% 26% 60%

Base: 2,190 global IT and business decision makers with involvement in setting strategy for data initiatives at their organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of KPMG International, July 2017

Sources

[1] 2015 Intangible Asset Market Value Study, Ocean Tomo

[2] LSE Business Review, 2017

[3] *Findings Regarding The Market Events of May 6, 2010*, 30 September 2010, America's Securities and Exchange Commission and its Commodity Futures Trading Commission

[4] ARS Technica, 2016

[5] *Four ways Google will help to tackle extremism*, 18 June 2017, Financial Times

[6] Sheryl Sandberg, Facebook post, September 2017

[7] The next Web, 2017

[8] *Facebook enabled advertisers to reach 'Jew Haters'*

[9] Reuters, 2017

[10] Social and Economic Sciences, 2014

[11] Quartz, 2017 (Quartz, 2017)

[12] Partnership on AI to Benefit People and Society

[13] Google

[14] http://www.dataversity.net/evolution-data-preparation-data-analytics/

About Intelligent Automation and Data & Analytics at KPMG

In a global environment defined by constant disruption, business leaders need technology they can trust to inform their most important decisions. KPMG's Intelligent Automation and Data & Analytics (D&A) team has earned that trust with an evidence-based, business-first approach that's at our core. For more than 100 years, KPMG professionals have worked across industries to help clients address their long-term, strategic objectives. And as an internationally regulated accounting and professional services network, member firms have an unwavering commitment to precision and quality in everything they do. For more information, visit kpmg.com/trust.

Contributors

Dr. Thomas Erwin
Global Head of KPMG Lighthouse
Center of Excellence for Data & Analytics and Intelligent Automation
Partner, KPMG in Germany

Thomas drives the growth of the global Data & Analytics practice. Since 2002, Thomas has worked with numerous KPMG global clients, helping them find the right Data & Analytics (D&A) approaches and solutions, including the implementation and worldwide roll-out of respective tools
and technologies.

Brad Fisher
Data & Analytics Leader, US, KPMG International
National Leader D&A, KPMG in the US
E: bfisher@kpmg.com

As the D&A Leader for KPMG in the US, Brad has presided over the firm's rapid growth in the scale and range of advanced capabilities of the firm's Data & Analytics services. Under his leadership, the KPMG Lighthouse was created as the firm's D&A Center of Excellence, housing close to 300 advanced data scientists and Big Data software engineers in the US. Brad works with clients to help them unlock the value of AI by providing insight on what tools to innovate with and how to implement sustainable processes built on AI insights.

Anthony Coops
Data & Analytics Leader, ASPAC, KPMG International
Partner, KPMG Australia
E: acoops@kpmg.com.au

Anthony is the Leader of D&A for the Asia-Pacific region and head of D&A for the Australian member firm. A partner with KPMG Australia, Anthony has global experience working across multiple countries, where he helps clients address specific needs in areas such as risk, optimization, workforce and customer analytics.

Professor Sander Klous
Data & Analytics Leader, the Netherlands,
KPMG International
Partner, KPMG in the Netherlands
E: Klous.Sander@kpmg.nl

Sander is D&A Leader for KPMG in the Netherlands and professor in Big Data ecosystems for business and society at the University of Amsterdam. He has a PhD in high energy physics and worked for over a decade on a number of projects for CERN, the world's largest physics institute in Geneva. His best-selling book *We are Big Data* was runner-up for the management book of the year award in 2015. His new book *Trust in a Smart Society* is a top selling management book in the Netherlands.

Maurice op het Veld
Data & Analytics Leader, the Netherlands,
KPMG International
Partner, KPMG in the Netherlands
E: ophetveld.maurice@kpmg.nl

Maurice is the D&A Leader for KPMG in the Netherlands and
has 18 years' experience providing IT advisory and audit services to multinationals across industries. As well as managing the D&A team in the Netherlands, he is also responsible for a number of international clients, delivering advisory services. He is also a guest lecturer at the Tilburg University — TIAS School for Business and Society.

Murray Raisbeck
Data & Analytics Leader, UK, KPMG International
Partner, KPMG in the UK
E: murray.raisbeck@kpmg.co.uk

Murray is a partner within KPMG in the UK's Financial Services practice and the D&A lead in the UK. Murray also leads KPMG's Global FinTech network. He has worked with clients across the financial sector and the FinTech network that spans 31 countries in key FinTech hubs. An auditor by background, Murray works with global financial services clients in the insurance, asset management and wealth management industries. Murray's 18+ years of advisory experience includes finance change and regulatory programs, Sarbanes Oxley implementation projects, accounting advice on group reconstructions, Part VII transfers, and a variety of transactions.

Nadia Zahawi
Director, Global Data & Analytics
KPMG in the UK
E: nadia.zahawi@kpmg.co.uk

Nadia leads thought leadership for Global Data & Analytics based in the UK. Nadia works with both client-facing and internal KPMG teams to explore the value of emerging D&A solutions and capabilities. She has 20 years of experience working with leaders across multiple sectors to drive large-scale change, particularly with the UK government.

Contacts

Eva Garcia San Luis

Head of Data&Analytics and Artificial Intelligence

KPMG Spain

Tel. 914568219
evagarcia1@kpmg.es

José Ángel Alonso

Director, Data&Analytics and Artificial Intelligence
KPMG Spain

Tel. 914513249
joseangelalonso@kpmg.es

Acknowledgements

Additional references

KPMG — Embracing the cognitive era. Using automation to break transformation barriers — and make every employee an innovator

KPMG — An ethical compass in the automation age. Decisions require deep dive into company core values

KPMG — Rise of the humans. The integration of digital and human labor

KPMG — Bots in the back office. The coming wave of digital labor

KPMG — Accelerating Automation. Plan your faster, smoother journey

KPMG — Mit Daten Werte Schaffen. Report 2017

kpmg.com/trust

kpmg.com/data

kpmg.com/socialmedia