Deloitte.

MAKING AN
IMPACT THAT
MATTERS
since 1845

See the Unseen
Global Digital Risk
Survey 2022

MAKING AN
IMPACT THAT
MATTERS
since 1845

Contents

The digital confidence gap

All organisations need a social licence to operate. To function effectively, they require approval and acceptance of their interactions with and impact on consumers, stakeholders and society. This has never been truer than in the digital era.

Digital technology has already transformed the way business is done and continues to do so in a ceaseless, disruptive revolution. Businesses are constantly being challenged by competitor and consumer expectations to 'keep up'. They are also continually challenging themselves to further digitise to increase organisational efficiency, improve routes to market, and enhance customer experience.

As digital transformation accelerates, the question of ethics has become even more prevalent. It is therefore vital that consumers have confidence that the use of those digital technologies to deliver products and services is safe, secure and sustainable. Ultimately, do they feel their best interests are at heart?

Unfortunately, that is not always the case. This survey finds a substantial gap between consumer confidence in digital technologies and the confidence that business leaders place in them. In turn, this translates into a confidence deficit, putting the social licence to operate in jeopardy.

Just 22% of consumers declare themselves '**highly confident**' regarding the use of digital technologies in this context compared to 40% of leaders.
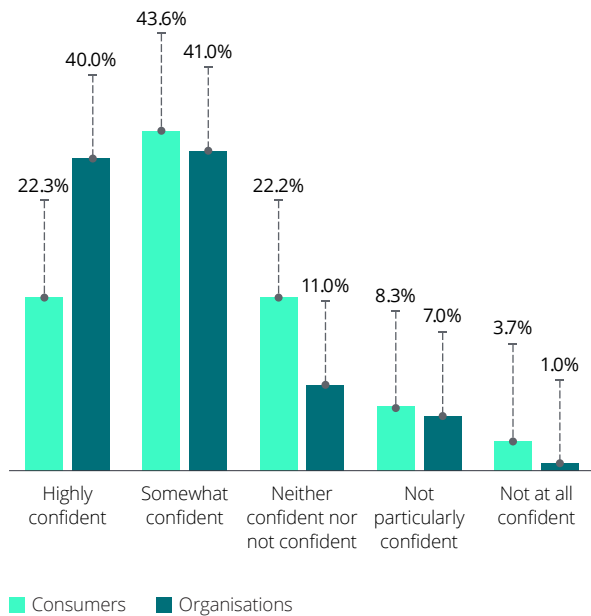
Even when those who are merely '**somewhat confident**' are considered, the disparity remains; the net confidence level among consumers increases to 66% but still lags considerably behind the comparative figure for business leaders at 81%.

The Global Digital Risk Survey 2022 'See the Unseen' analyses confidence in digital technologies amongst consumers and organisations. Specifically, it explored sentiments and experiences around the safety, security and sustainability of digital technology, the risks induced by such technology, the repercussions and concerns of digital incidents and the responsible and accountable business leaders. Over 1,000 business leaders and 5,300 customers were interviewed, across financial services, the public sector, consumer products and many more industries. Input was gathered on an industry-wide and global scale – from APAC and EMEA to UK and the Americas – looking to determine the state of, and how to build, digital confidence.

"We cannot allow these harmful behaviours and content to undermine the significant benefits that the digital revolution can offer. While some companies have taken steps to improve safety on their platforms, progress has been too slow and inconsistent overall."

Online Harms White Paper – GOV.UK (www.gov.uk)

How confident, or not confident, are you that digital technologies are safe, secure and sustainable?

	Highly confident	Somewhat confident	Neither confident nor not confident	Not particularly confident	Not at all confident
Consumers	22.3%	43.6%	22.2%	8.3%	3.7%
Organisations	40.0%	41.0%	11.0%	7.0%	1.0%

The existence of this gap has clear implications for the future success, and even viability, of transformative and innovative corporate digitisation strategies – including those that deploy artificial intelligence (AI), cloud, automation, machine learning, and data analytics. For every digital decision made risk must be considered.

At its simplest, this means looking at how to make the digital unknown unknowns visible and make a conscious decision about how to manage their implications. Doing this proactively will build confidence/reassurance that the desired output is being reached effectively. It will also help to bridge the confidence gap. But beyond this, it provides the opportunity to differentiate; by seeking new ways to develop your digital footprint, it maximises the commercial and societal value of digital as well as augmenting reputation.

Responding effectively means seeking answers to certain key questions:

- Why does this gap occur? Is this a case of perception or reality? Or are the actions taken by organisations to protect consumers simply going unseen?

- Is the gap more about inherent trust in the organisation itself or trust in the underlying technology applications?

- Who is really in control? What is the interplay or interaction between consumer, organisation and technology?

It is these themes that we explore in this report.

Key findings

The digital confidence gap

Are digital technologies used to deliver products and services
safe, secure and sustainable?
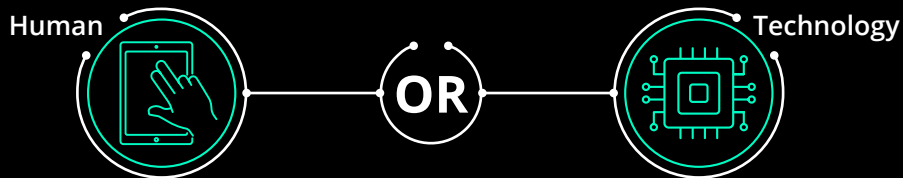
✓ **Strongly Agree**

40%
of business leaders

22%
of consumers

Why does this gap occur? Is this a case of perception or reality? Or are the actions taken by organisations to protect consumers simply going unseen?

To bridge this gap we need to identify and amplify the drivers of digital confidence.

Who's in control?

Human **OR** Technology

We compared consumers' confidence in technology to carry out 26 daily activities.

Banking   Healthcare   Driving

Security   Entertainment   Retail   Sentencing
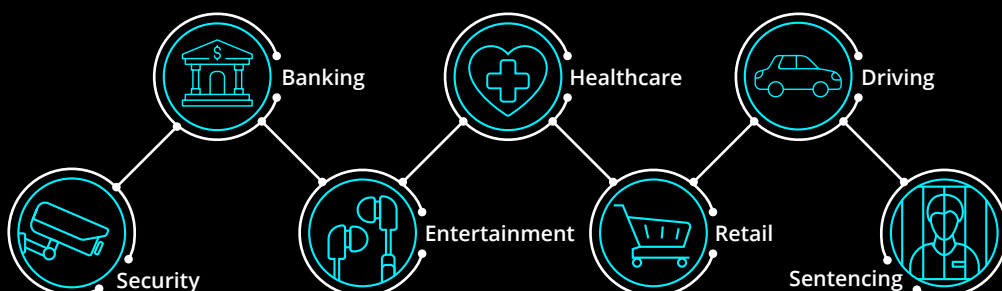
People are happiest using technology when they feel ultimately in control of it.

How to help consumers feel in control:

1
Provide immediate assurance that an activity has happened as desired

2
Enable people to retain power to make the ultimate decision

3
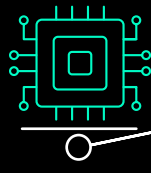Adapt consumer experiences depending on the perceived risk involved

Consumer experience – The biggest digital risk?

Only 2/10 digital incidents reported over the last year **related to the technology itself.**

The biggest digital incident reported was **failure of customer services to help with a technology problem.**

Are you investing **too much in technology?**

and **not enough in people?**
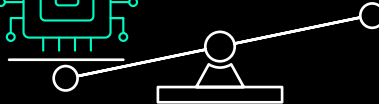
Consumers identified three factors which are vital to building confidence in digital, but are falling short of expectations:

Transparency

60%

don't feel adequately informed by organisations about how they use digital technologies

Regulation

55%

agree increased regulatory oversight is needed

Ethics

60%

don't think organisations follow digitally ethical practices

Who's responsible for digital risk in your organisation?

CDO

CTO

CRO

75%
feel confident to identify
and manage digital risks
in their role.

CIO

CEO

But there's no clear and single owner for digital risk.

How can you bridge
the digital confidence
gap?

Embed risk and controls across the
organisation so they enable **security,
safety and sustainability** across
digital decision making, and don't
impede innovation.

Chapter 1

Human v technology – who's in control?

The business world has embraced digital transformation at scale and at pace over the last five years. Digitisation is now pervasive rather than niche, mainstream rather than an outlier.

"Digital, the word, will disappear. It's ubiquitous."

Tom Bigham, Digital Risk Partner

What's next? The distinction between digital operations and business-as-usual will disappear, as with the term 'e-commerce' in the wake of the dot-com era.

Mirroring the early days of the commercial internet, digital technologies will cease to provide the competitive edge in themselves, but they will emerge as the arenas in which companies compete.

Without confidence it is very difficult to conduct business or engage with consumers. Digital ethics, the responsible use of data and digital technology by organisations, is paramount in earning that confidence whether that is in terms of privacy, data-sharing, responsiveness, transparency, fairness, sustainability, or the other values prioritised by consumers.

Given the premium put on trust in customer relationships, business leaders should be concerned that less than half of respondents think that businesses follow digitally ethical practices and just 37% feel that they are adequately informed by those organisations about how that digital technology is being used.

< 50%
of consumers feel that organisations follow digitally ethical practices

This confidence deficit contrasts sharply with the views of business leaders; more than three-quarters (78%) of whom are confident that their organisations follow digitally ethical practices. In fact, more than a third are highly confident (36%) compared to just one in seven (15%) consumers.

The confidence disparity between consumers and organisations indicates that organisations face a dilemma balancing digital strategies they are pursuing with what consumers are comfortable with.

But the devil is in the detail, drilling down into the survey results – across 26 use cases of digital technology – produces striking insights. Interestingly, issues of control predominate, as consumers discover that the face-to-face human interactions they are used to are being replaced by sometimes invisible algorithms.

How confident are consumers in the use of digital technologies to carry out activities?

MOST

66%
Would make payments/transfer using a banking app/website

62%
Would shop for low/medium value items on retailer's app or website, opposed to in stores e.g. clothes, groceries or technology

60%
Would control home heating, lighting, security or music using digital assistants such as Smart home technologies

LEAST

38%
Would not use AI-driven medical treatments and diagnoses

35%
Would not use autonomous vehicles, including cars and planes

32%
Would not use AI to provide judicial judgements and sentencing (including criminal)

"We often talk about the head v heart dilemma of digital risk. The head; digital innovation is driven by demand for business growth, competition and commerciality. The heart; this is far less objective – driven more by consumers perception of and preferences for digital innovation."

Charlie Gribben, Digital Risk Partner

People are happiest using technology when they feel that they are ultimately in control of it. The more authority that the human actor has to override or cancel a digital process, whilst having the option to interact with another human, the more confident they are. Quite simply, we need to find that equilibrium between full digitisation and human control. This confidence can be greatly enhanced by ensuring that three behavioural traits are respected:

"What sources of proof or safety exist?"

Tom Bigham, Digital Risk Partner

1. Providing immediate assurance that an activity has happened as desired and transparency of the repercussions: Anyone who has used a digital technology is all too familiar with that queasiness that comes from not knowing whether a process or transaction has been successfully completed. When wi-fi connection is lost just as the app is processing a payment, consumers want to get immediate assurance that the activity took place as desired. Transparency is paramount, as is the hybrid of technical excellence and the resilience provided by human back-up.

2. Enabling humans to retain the power to make the ultimate decision: Comfort with reliance on digital technologies has increased enormously; for example, recent years have witnessed the rapid rise in popularity of voice controlled virtual assistants. AI is transforming data-heavy industries such as finance, retail and healthcare – in beneficial and positive ways.

3. Adapt consumer experiences depending on the perceived risk involved: Trust and confidence are greatly enhanced when the nexus of human, machine, risk and confidence are in harmonious balance. The survey results point to a sweet-spot in digitisation that exploits the machine capabilities in making recommendations and process efficiency while leaving the human actors with control and transparency over the final decision and outcome.

This is clearly seen in the fact that nearly half (46%) of consumers are confident to allow digital technologies to monitor vehicle safety whereas this falls to just over a third (35%) who are confident in letting AI ultimately control an autonomous vehicle. The same psychology pertains in financial decision-making.

While 57% would be confident in letting a bot analyse their personal data to make investment recommendations, this falls to just 40% of consumers who would be confident in letting the same technologies manage their portfolios.

Considering the degree of impact if something goes wrong, asking ourselves 'what's the worst that could happen?' is a key heuristic for humans. In the digital context, people tend to be much less confident in those technologies that could potentially have a high impact on their lives.

That can be seen in the relatively high levels of confidence in allowing automation of low impact, routine tasks such as making online payments (66%), shopping for low value items (62%) and controlling home heating and lighting (60%).

The flipside of this confidence is the relative aversion to ceding control to digital applications, when the stakes are much higher in terms of potential negative consequences if an error is made. Hence, just 38% of consumers are confident in letting AI make medical diagnoses or recommend treatment while less than 32% are confident in letting an AI application decide judicial sentencing.

Such issues of trust in the emerging digital ecosystem are not intractable. More than half of consumers (55%) would feel more confident in using digital technologies if a regulator had more authority and oversight. The confidence with which organisations are addressing these regulatory and legal requirements varies significantly across industry. Banking (80%), manufacturing (70%) and education (70%) are among the most mature compared with oil and gas (47%), energy (44%) and life sciences (38%) among the lowest.

"GDPR shone a light on how much we inherently trust organisations. But even some of the most advanced struggled to deal with the implications. Regulation should focus on enabling organisations, and helping the demonstrate positive outcomes."

Charlie Gribben, Digital Risk Partner

How regulatory change can drive consumer confidence?

Consumer-led design: Embedding regulatory objectives in digital journeys; Suchitra Nair, Partner EMEA Centre for Regulatory Strategy

"There are two fundamental ways that consumer confidence in digital can be built by applying regulatory objectives. Organisations have the opportunity to differentiate and this is actionable **now**.

1. Most organisations apply regulations as an after-thought, and layer it over the design of the digital customer journey. This can lead to the customer not fully understanding the risks, protections available, or costs inherent in that service. This will inevitably lead to a confidence gap if any of those risks manifest or perceived protections are not made available. Lessons can be learnt from successful digitally native fintechs who have adopted a regulation-first approach, integrating it fully in the customer journey, and prioritising transparency and clarity of terms and protections and building in optionality for the consumer to actively choose the risk/cost trade-offs through the digital journey.

For example, during a digital car insurance application process, at an early stage in the journey a customer can choose to add breakdown cover at an extra £20. The risk/cost trade off is clear up front and optionality is available, putting the customer in control and being clear about the level of protection available.

The design challenge of course is striking the balance between clarity, optionality and delivering a seamless customer experience.

2. As digitisation becomes more pervasive in the market, expectations around value, suitability, access and transparency have increased from both customers and regulators. Additionally, particularly in financial services – but increasingly in other sectors – firms are being held accountable for treating customers fairly. Catering to a diverse set of customers, including those that are vulnerable, and ethical use of data are increasing in importance. While regulation sets the expectations of how these critical areas should be addressed, firms who embrace these concepts into the DNA of their strategy will successfully differentiate themselves in the market and bridge the consumer confidence gap."

The Future of Internet Regulation: Compliance as a Competitive Advantage; Nick Seeber Internet Regulation Lead Partner

"As the world has become connected, the same challenges we see in the real world – harmful and antisocial behaviour, misinformation and crime – are now unconstrained by national borders, able to spread instantly and impact many more people.

How do organisations retain and build consumer confidence as digital use increases and new challenges continue to evolve? How do regulators and internet companies ensure consumers feel in control and not more exposed?

Naturally, policymakers are looking to ensure the Internet is a safe and open space for everyone. Comprehensive regulation of the online business environment has the potential to provide control and transparency to consumers and strengthen not only internet company brands but also how all organisations use the Internet. Providing internet companies

with "rules of the road" gives these organisations standards and guidelines to adhere to, instead of having to self-regulate and be held accountable to undefined standards by governments. It also empowers consumers to take control of their online presence and the way they interact with organisations' content on these platforms.

However, this regulatory wave requires internet companies to transform the way they operate and engage in the complex interplay of trust, safety and open competition. They must elevate and integrate risk and compliance to their core agenda."

Deloitte's "The Future of Internet Regulation: Compliance as a Competitive Advantage" whitepaper explores these challenges and outlines our six critical actions that can shift regulatory response from a posture of defence to advantage.

The fundamental shifts in the way that risk manifests in a digital organisation will certainly require new risk, compliance and control frameworks. An agile approach that allows monitoring of risks in real-time, rather than introducing more friction, would ultimately benefit all parties.

But there is a balance to be achieved between introducing more regulation, ensuring better compliance with existing regulations, and simply improving transparency and communication around digital risk generally.

55%

of consumers agree that **increased regulatory oversight** would improve their digital confidence

Tellingly, only 40% of consumers currently feel adequately informed by organisations about their digital policies, suggesting that more openness and consumer engagement would be a quick win in addressing the trust gap.
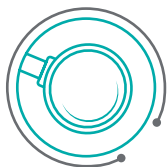
60%

of consumers don't feel adequately **informed** by organisations about their use of digital

How to bridge the confidence gap?

As companies continue to digitise, building confidence also means ensuring control over technology both internally and externally. Control in this instance doesn't just refer to the guardrails put in place by an organisation to manage risk, it requires cooperation between many different players and relies on pre-emptive communication between them. Consider:

- What can you learn from the experiences of other sectors and organisations?

- How can you make sure that you have identified the right risks to manage?

- When developing automated services and solutions, have you stress-tested the confidence that consumers would have in them and your organisation? Before undertaking any new digital innovation – have you thoroughly mapped the impact to customer experience?

- How are you communicating with customers to give them the confidence that they are in control by embedding transparency, choice and fairness in everything you do?

- Are you prepared for the upcoming set of regulatory interventions across the digital landscape? Who in your organisation is responsible for responding to the same across the end-to-end customer journey?

Digital brings new unknown unknowns, creating new risks for organisations. Being able to identify, assess and remediate these risks can give stakeholders the confidence that digital risks will not turn into digital issues.

Chapter 2

Consumer experience – the biggest digital risk to your business?
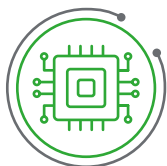
Digitisation has accelerated as a result of the Covid-19 pandemic. But while technology changes rapidly, people don't. No matter how sophisticated the AI and robotics enabling them, services need to remain human-centric and customer-centric.

However, over the last year, more than half (52%) of consumers report feeling more at risk in the digital environment following the lockdown-induced rapid shift to working, shopping, and socialising online. Suddenly everything from consulting our GPs to watching concerts was happening digitally.

Business leaders share this perception, with a similar proportion (55%) recognising the greater risks.

52%

of consumers feel more at risk when using online services due to accelerated digitisation prompted by the Covid-19 pandemic

While 72% of consumers have experienced an adverse digital incident in the last year, just two out of the top ten reported incidents related to issues with the technology itself. The majority concerned problems with the interaction between humans and technology.

The most prevalent issue was customer services being unable to help the consumer with a problem (23%), indicating that failure to provide human support is more annoying than technology failure.

However, the second-most widely reported risk event from a customer perspective was feeling 'uncomfortable about the level of oversight that organisations have of me' (19%). This suggests that the limits on surveillance may be approaching and that consumers will be disinclined to engage with businesses where the relationship is seen as asymmetrical and exploitative.

For all the sophisticated technology behind it, excellence in customer experience remains dependent on very human interaction. Digital – in the form of cloud, artificial intelligence, and automation – simply helps organisations to meet and exceed their customers' ever-increasing expectations. People need to be able to step into a process and resolve issues when the technology fails.
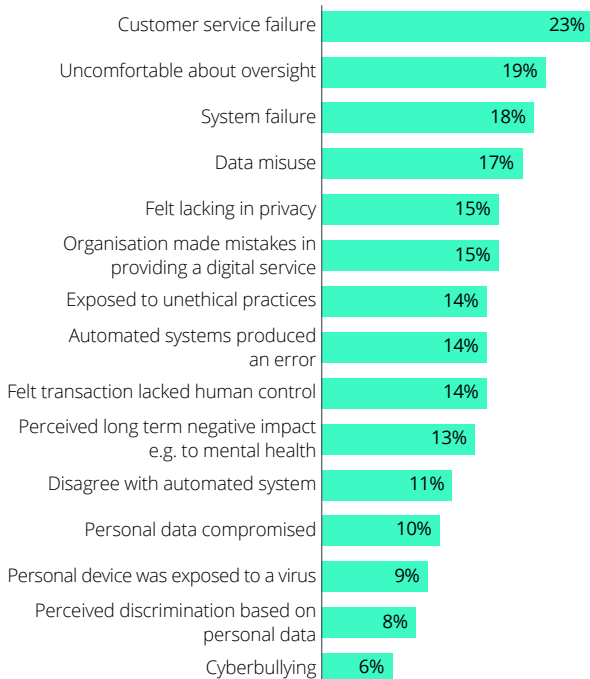
"Are we over-investing in technology, and not enough in people?"

Charlie Gribben, Digital Risk Partner

Even in the brave new world of automation, digitisation and cloud, the objectives of great customer service are what they always have been: speed, personalisation, efficiency and convenience, backed by highly effective resolution of problems. Getting that right is front and centre of any consumer-centric digital strategy.

Being proactive in addressing issues, incidents and problems can actually enhance organisational reputation and customer approval if the process is handled well. Failure to deliver on those imperatives is arguably the biggest risk facing consumer-facing organisations, as the survey reveals.

Over the past 12 months, which of the following, if any, have happened to you whilst using digital technologies?

Customer service failure	23%
Uncomfortable about oversight	19%
System failure	18%
Data misuse	17%
Felt lacking in privacy	15%
Organisation made mistakes in providing a digital service	15%
Exposed to unethical practices	14%
Automated systems produced an error	14%
Felt transaction lacked human control	14%
Perceived long term negative impact e.g. to mental health	13%
Disagree with automated system	11%
Personal data compromised	10%
Personal device was exposed to a virus	9%
Perceived discrimination based on personal data	8%
Cyberbullying	6%

How to bridge the confidence gap?

Customer experience needs to be at the forefront of your digital strategy – from the level of insight into customers to the support given to them. Achieving that requires consideration across areas, including:

- Are you building world-class customer experiences that blend seamless automation with a human touch?

- Are your risk functions involved in the customer experience design process?

- How do you make technology feel human when that is what customers require?

- How do you ensure that the digital and human elements are optimised in your consumer experience?

Digital transformation is not just about technology, but also about the longer term considerations on people and process. We help devise actionable strategies embedded with a holistic approach to risk, and deliver customer-centricity.

Business leaders feel in control, but are they?

Business leaders are feeling positive about their digital risk management capabilities. Perhaps too positive, since the evidence suggests they are vastly underestimating the repercussions of digital incidents.

Three quarters of business leaders (75%) are confident in their ability to deliver on their responsibilities when it comes to identifying and managing digital risks, albeit only a third (35%) express full confidence.

Such levels of assurance represent a remarkable sea-change in attitudes in a relatively short timeframe: our 2019 Global Risk Survey found that just 19% of leaders felt confident that their team had the right combination of skills and talent to effectively manage digital risk.
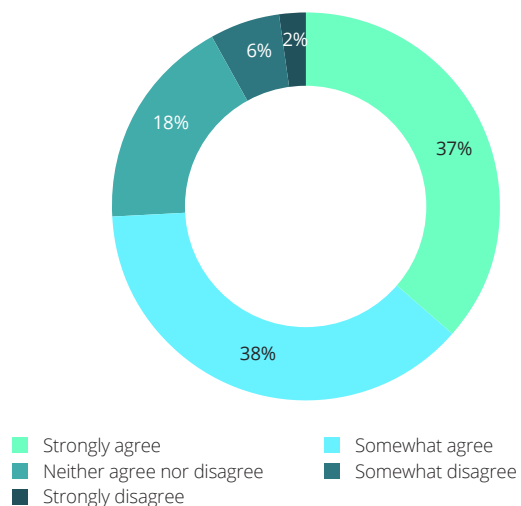
This new-found confidence extends to their perceptions of their performance, with four in five (79%) believing they have achieved the desired value or return on investment (ROI) from their digital transformation activities in the last 12 months.

While nearly half (46%) express concern that the digital dividend, in the form of value creation, is taking longer than expected to materialise, this nevertheless indicates a step change from the state-of-play reported in our 2019 Global Risk Survey.
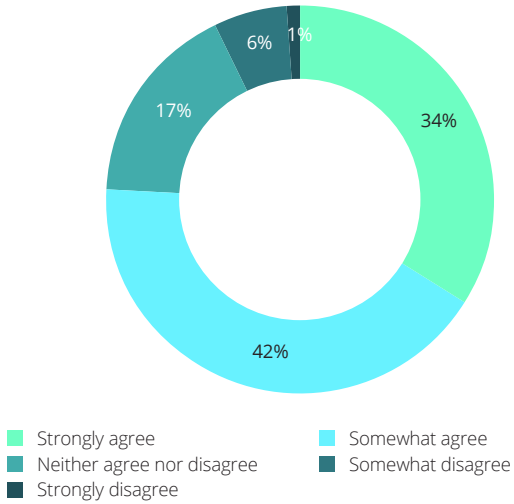
At that point, just 40% of organisations were adopting digital technology at scale. The impetus to accelerate digital transformation generated by the pandemic is a contributory factor to this.

However, benchmarking against consumer perspectives suggests that this confidence around digital risk may verge on hubristic at times.

Identifying – I am fully aware of the breadth of digital risks I need to be responsible for

- Strongly agree
- Somewhat agree
- Neither agree nor disagree
- Somewhat disagree
- Strongly disagree

37%
38%
18%
6%
2%

Managing – I feel confident I can address the breadth of digital risk I need to be responsible for

- Strongly agree
- Neither agree nor disagree
- Strongly disagree
- Somewhat agree
- Somewhat disagree

Consumers are far from passive when it comes to their reaction and response to being exposed to digital incidents. Instead, they proactively seek restitution and redress. More than two in five (43%) would stop engaging with an organisation or switch suppliers while a third (33%) would report an organisation to the regulator.

Worryingly, just 15% of business leaders have identified and acknowledged the risk of customers abandoning them as the result of digital incidents.

This failure to anticipate or mitigate digital risks has clear implications for the functioning of organisations, given the potential to create adverse impacts on customer experience, society, operational efficiency, profitability and public reputation.

In the past 12 months, have you felt that your business is achieving the desired value and or return on investment (ROI) from your digital transformation?

- Yes
- Somewhat
- Yes – but it has taken longer than expected
- No
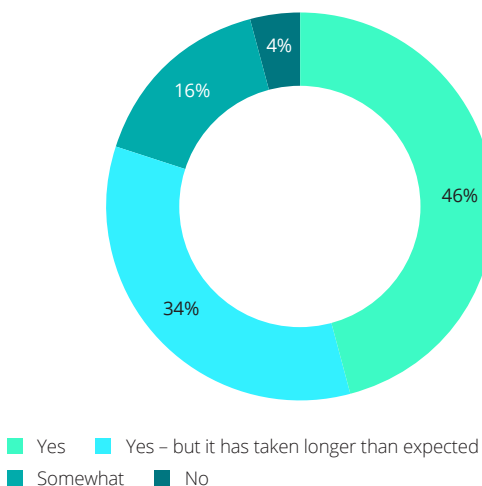
Ownership and management of digital risk

Since digital risk first emerged as a separate category in the corporate risk register, no definitive best-practice model for managing, monitoring and mitigating it has prevailed.

Patterns of ownership of digital risk remain hugely varied and idiosyncratic from organisation to organisation. This reflects the unique characteristics of each individual organisation's digital transformation journey and adoption strategies, as well as their cultures and legacy structures.

Our survey confirmed this disparity by revealing a striking lack of consensus. While 19% of organisations saw the chief technology officer (CTO) as being responsible for digital risk, 17% felt that ultimate ownership resided with the chief digital officer (CDO). Meanwhile, 16% believed that the chief information security officer (CISO), should lead compared with 15% who saw it as the remit of the chief information officer (CIO). Positively, only 1% of respondents were unsure about who owns digital risk, which is a significant change from the 12% giving the same answer in our 2019 survey.

In a sense, all views are correct. With digital now integral, rather than peripheral, to all aspects of a business, risk management models are adapting. Ideally risk controls associated with digitisation should be automated, embedded in the organisation and fully aligned to business goals.

However, when asked how mature their organisations were across a spectrum of core digital risk capabilities, more than a third of business leaders (34%-39% depending on capability) acknowledged that they were either not mature, still scoping, or had simply not considered the risks.

Arguably, the greatest obstacle to successful digital risk management is failure to recognise that digital is not just the technology – it's also the people, the processes and the interaction points that facilitate it. Yet, perhaps counter-intuitively, less than 5% of organisations currently place ownership of digital risk with the risk team.

Forward-thinking organisations are recognising the need to accelerate the introduction of controls so that they do not lag too far behind and impede digitally-enabled operational innovations. They take an agile approach, hiring and embedding a new generation of risk managers who more intrinsically understand the digital landscape and the opportunities it presents.
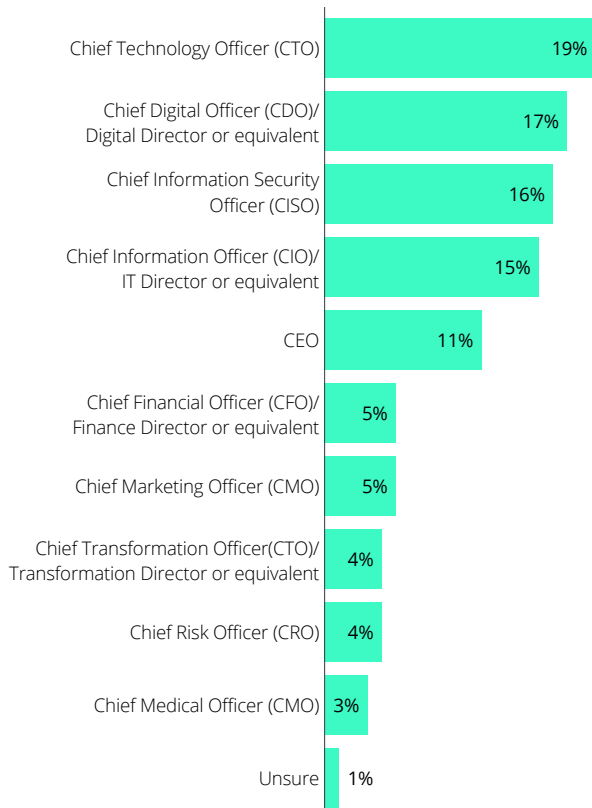
"The difficulty for risk and compliance teams is that digital means they can't provide confidence or assurance in the way they traditionally did. Things are more joined up now and happen at extreme pace and scale."

Tom Bigham, Digital Risk Partner

Digitisation will continue to be interwoven into the fabric of business until it is seamless and indivisible. Those organisations that manage the process effectively and quickly will emerge as winners.

Best practice in risk and control will evolve from viewing digital risk as a new, separate and discreet risk category to taking a systemic, enterprise-wide approach to managing all risks associated with digitisation.

In your organisation, who is responsible for leading the identification and management of digital risk?

Chief Technology Officer (CTO)	19%
Chief Digital Officer (CDO)/ Digital Director or equivalent	17%
Chief Information Security Officer (CISO)	16%
Chief Information Officer (CIO)/ IT Director or equivalent	15%
CEO	11%
Chief Financial Officer (CFO)/ Finance Director or equivalent	5%
Chief Marketing Officer (CMO)	5%
Chief Transformation Officer(CTO)/ Transformation Director or equivalent	4%
Chief Risk Officer (CRO)	4%
Chief Medical Officer (CMO)	3%
Unsure	1%

How to bridge the confidence gap?

Establishing a business structure and culture which ensures digital risks are both managed and controlled is key.

• Who is responsible for the governance and management of digital risks across your organisation and do they have the right level of information they need?

• Do you have a business-led but risk aware culture that will allow you to manage digital risks effectively?

• Are your controls aligned to business goals and appetite?

We work hand-in-hand to get to know teams across the business and understand every organisations, unique ecosystem. By helping to establish the right roles and responsibilities to align with digital strategy we can develop an integrated holistic and agile digital risk strategy that builds confidence and value through digitisation.

Contacts

UK Digital Risk Leads

Charlie Gribben
Digital Risk Partner
Consumer and Public Sector

Tom Bigham
Digital Risk Partner
Financial Services

Dimi Milanov
Senior Manager
Digital Risk

Madeleine Thirsk
Manager
Digital Risk

Specialist Contributors

Nick Seeber
Lead Partner
Internet Regulation

Suchitra Nair
Partner
EMEA Centre for Regulatory Strategy

Jennifer McMillan
Manager
Internet Regulation

Global Leaders

USA

Adam Thomas
Partner
Risk and Financial Advisory

Adam Berman
Partner
Risk and Financial Advisory

Stuart Rubin
Managing Director
Risk and Financial Advisory

Gina Primeaux
Partner
Risk and Financial Advisory

Canada

Don MacPherson
Partner
Risk Advisory

Baskaran Rajamani
Partner
Risk Advisory

Judit Halin
Partner
Risk Advisory

Spain

Manel Carpio
Partner
Risk Advisory

Elisa de Hevia Gisbert
Partner
Risk Advisory

Netherlands

Marko van Zwam
Partner
Risk Advisory

Harold Malaihollo
Partner
Risk Advisory

France

Gregory Abisror
Partner
Risk Advisory

Antoine Gajac
Partner
Risk Advisory

Germany

Martin Flisgen
Director
Risk Advisory

Stefan Steinhoff
Partner
Risk Advisory

Australia

Darren Gerber
Partner
Risk Advisory

Japan

Yasuhide Onuma
Partner
Risk Advisory

Tomotake Kozu
Partner
Risk Advisory

Singapore

Mark Woodley
Partner
Risk Advisory

China

Rebecca Wei Jiang
Partner
Risk Advisory

Allan An Xie
Partner
Risk Advisory

Deloitte.