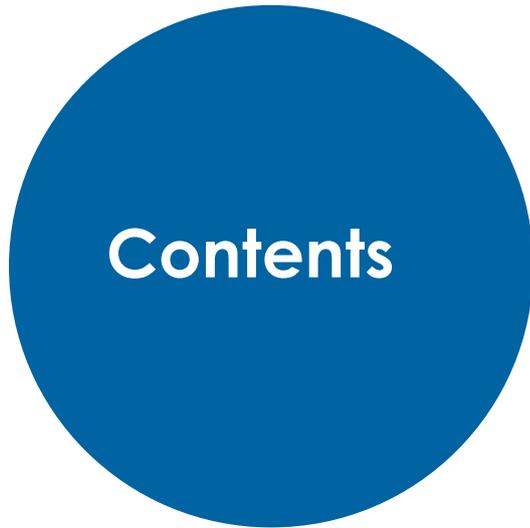


Cloud complexity: The need for resilience



Sponsored by





Contents

Preface	2
Introduction	3
1 Resilience and the cloud	5
2 The building blocks of cloud resilience	8
3 Conclusion: mindsets and partnerships for resilience	12
Appendix: survey results	13

Preface

Cloud computing has helped reduce costs and boost productivity at many organisations, but its broader use brings both benefits and risks. These risks extend well beyond security breaches into a lack of oversight of complex, often fragmented systems that, if not managed well, limits an organisation's ability to capture new opportunities and to adapt and respond to new technology or regulatory controls.

How should Chief Information Officers leverage the cloud's potential? How can they fortify their company's continuity and agility in the cloud? What key challenges must be overcome to succeed on this journey? Like all big changes, a successful shift to cloud computing requires a shift in both mindsets and strategies, processes and partnerships across and outside a company.

This report by the Economist Intelligence Unit

(EIU) on behalf of Sungard Availability Services explores these and other critical questions as companies expand their cloud use.

The findings and views in this report do not necessarily represent the views of the sponsor. The author is Peter Moustakerski; Carolyn Whelan edited the report. We would like to thank all the executives who participated on the record and anonymously.

Interviewees

- Kristin Darby, chief information officer, Cancer Treatment Centers of America
- Dom Guinard, co-founder and CTO, EVERYTHING
- Tanuja Randery, president UK & Ireland, Schneider Electric
- Harsh Sinha, vice president, Engineering, TransferWise

Who took the survey?

In March of 2016, the EIU, for a research programme sponsored by Sungard Availability Services, polled 304 executives evenly dispersed across France, the United Kingdom and the United States on their organisational resilience and technology adoption. Respondents hail from a number of industries, including IT and technology (15%), financial services (13%), professional services (8%), manufacturing (7%) and 15 other sectors (collectively 57%). Those polled hold the titles of chief information officer (50%), senior vice president (12%), vice president (15%) or head of IT (23%). The companies they represent earn between \$50m and \$500m (45%), or more than \$500m (55%) in annual revenue. ■

Introduction

Organisations today operate in an increasingly interconnected and information-rich world. Innovations like big data and dynamic pricing create unprecedented opportunity for businesses to launch novel products and services, conquer new markets and better engage customers. But the same developments bring new risks and challenges—from security breaches and service interruption to managing fragmented IT systems, vast data troves and the dizzying speed of change.

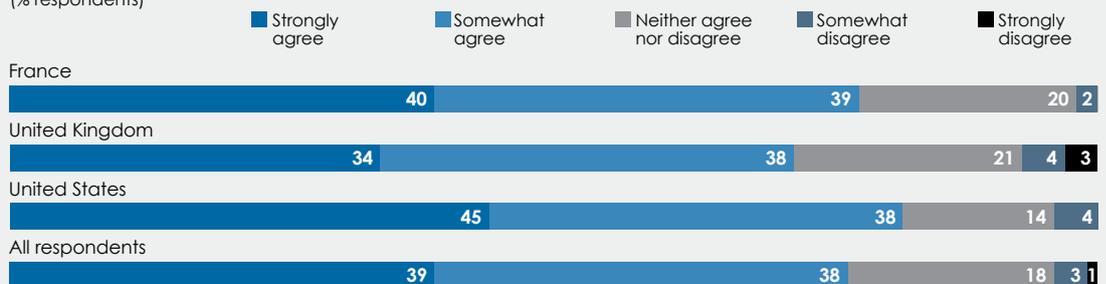
Cloud computing is perhaps the most prominent example of recent disruptive technologies that are reshaping corporate strategies and IT capabilities. Cloud use is now almost universal among organisations—and only expected to grow. In the EIU survey, 78% of executives agree that their use of cloud

computing will increase in the next three years (see Figure 1); nearly two-thirds (65%) say that more than half of their organisations' systems are now cloud-based versus the just 6% who say that one-quarter or less of their systems are in the cloud. "Companies are no longer considering whether to migrate to the cloud, but rather what ... and how best to migrate," notes Tanuja Randery, president, UK & Ireland at French electronics conglomerate Schneider Electric.

The move to the cloud is a logical one. Cloud solutions help organisations add new IT capabilities and applications at lightning speed, often at a lower lifetime cost. But the cloud can introduce more external players and potential breakage points that demand responses to both innovation and regulation at a faster pace than many IT organisations can meet.

Figure 1. To what extent do you agree with the following statement: "Our use of cloud computing will increase in the next three years"?

(% respondents)



Source: Economist Intelligence Unit, 2016.

Against this backdrop of change and uncertainty, “organisational resilience” is emerging as a critical lever of a successful cloud expansion. BSI, the business standards company, defines resilience in its newly published BS 65000 standard as the ability to both quickly bounce back from a major disruption and to “anticipate, prepare for, respond and adapt to events—both sudden shocks and gradual change” to survive and prosper.

In fact, as Lyndon Bird, technical director at BSI points out in a recent *Continuity Central* article, the field of Business Continuity Management is reorienting its focus to organisational resilience. Business continuity strives to prepare an organisation for effective responses to sudden, major disruptions with minimal business impact. The business continuity agenda has also traditionally resided within the risk and compliance function which has struggled to gain broader

buy-in from other functions—primarily because it has been considered by other functions across the broader organisation as “not their problem”.

Organisational resilience, by contrast, alters the management posture from a reactive one to proactively anticipating and preparing for future disruption—and not just sudden cataclysmic ones, but also gradual strategic shifts. This more complex and difficult goal is intricately linked to an organisation’s overall business strategy and requires broader mobilisation of corporate capabilities across an organisation—from human resources managers to department heads to those who oversee supply chains. They will need to organise everything ranging from business processes to internal controls to capture value and mitigate the risk inherent in cloud opportunities. Thus, the resilience agenda is reaching the highest levels of an organisation. ■

1 Resilience and the cloud

The same shift in executive focus is taking place within cloud computing. As executives' experience and comfort level with the cloud grow, they are refocusing their attention beyond continuity onto the strategically important objective of resilience.

This trend is clearly shown in the EIU survey. Nearly three-quarters (72%) of survey respondents say the importance of organisational resilience will increase over the next three years (see Figure 2), a sentiment expressed even more strongly in the US (78%).

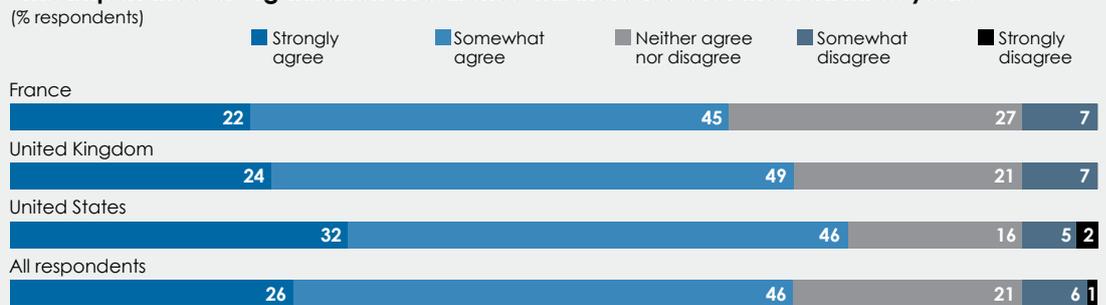
Notably, the more advanced a company is in its adoption of cloud technology, the stronger its focus on resilience appears to be. Respondents in the EIU survey who believe their organisation is ahead of its competitors in cloud adoption are nearly three times as likely

as the rest to also say they are ahead in their organisational resilience to technology risk. Indeed, according to respondents in the EIU survey, companies that are ahead of the competition in cloud adoption also tend to outperform their competitors in profitability and innovation. (See Figure 3).

On the other hand, the focus on resilience does not look to be linked to a company's cloud exposure. Survey respondents with just 1-24% of their IT assets in the cloud were just as likely to say that resilience will grow in importance as those who say that 75-99% of their IT systems are in the cloud (68% vs 70%).

To be sure, this is not a shift away from business continuity, which, like cloud computing, also focuses on the availability and security of IT assets—even more so in the

Figure 2. To what extent do you agree with the following statement: "The importance of organisational resilience will increase over the next three years"?



Source: Economist Intelligence Unit, 2016.

Figure 3. In your opinion, how does your company compare to its closest competitors in the following areas?

(% respondents)



Source: Economist Intelligence Unit, 2016.

age of the cloud. Security risks still top the list of cloud computing challenges identified by respondents in the EIU survey (see Figure 4), and are the most frequently named barrier to further technology adoption.

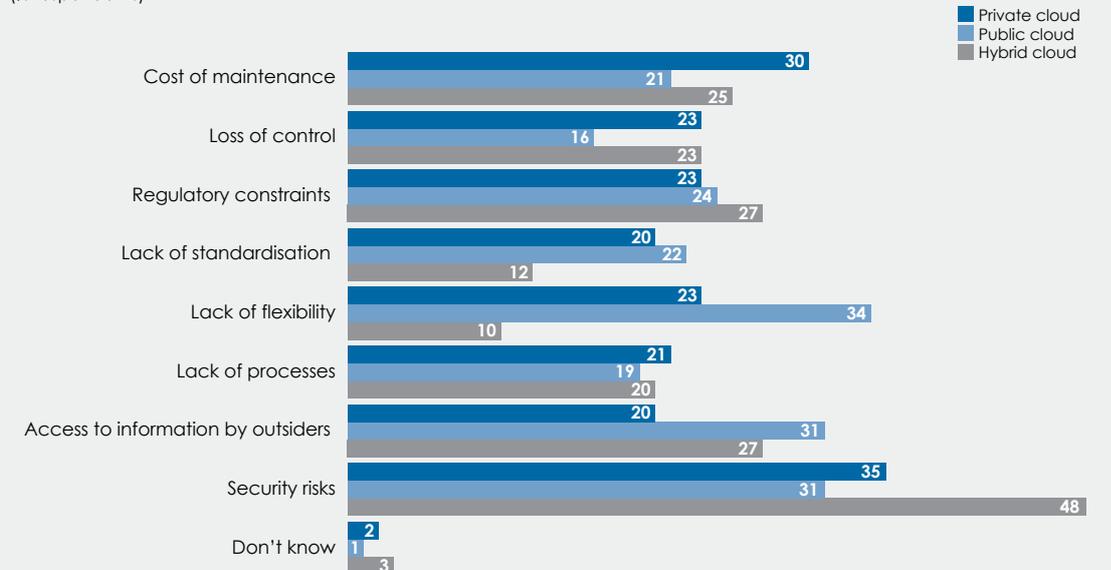
The most commonly cited risks are security breaches and leaks of confidential information (53% say they are extremely or moderately concerned about this risk), disruptions caused by cyber-attacks (52%) and potential failure to deliver product or services (46%). Two recent examples of high-profile security failure cases: breaches of federal workers' personnel files at the US

government's Office of Personnel Management and patient record breaches at CareFirst Networks.

"Both cloud providers and enterprises are getting smarter about security," observes Ms Randery of Schneider Electric. Indeed, no executive interviewed by the EIU for this report could recall any recent major disruption or incident pertaining to data security or service availability within their cloud systems. This reflects, perhaps, a growing view that data, systems and processes may be more secure with a large cloud provider than within a firm's own walls.

Figure 4. What are the top two challenges of your cloud computing approach?

(% respondents)



Source: Economist Intelligence Unit, 2016.

"It is much easier today to provide 100% uptime, so the cloud is actually a better place for security," seconds Dom Guinard, co-founder and CTO of technology company EVRYTHNG. He notes that cloud providers such as Amazon and Microsoft have invested heavily to address the security and stability challenges of their cloud environments, so companies are better off offloading these risks and responsibilities to large-scale providers. "On-premise is more risky," Mr Guinard cautions.

As the use of the cloud expands, executives are taking a more holistic and sophisticated approach, embedding the narrower goal of business continuity within the broader, more challenging and strategically relevant objective of organisational resilience. Ms Randery sums it up elegantly: "Resilience ... is not just about uptime and security; it is increasingly about agility, speed, multiplication and being more innovative." ■

2

The building blocks of cloud resilience

As organisations shift their focus from continuity to resilience, they will need to master the five key capabilities that follow. Although some of these building blocks are rooted in business continuity, they will need to be reshaped and reprioritised inside and outside a company to adapt to the new opportunities and risks that the cloud brings.

1. Specialised and regulatory requirements.

Migrating to one company-wide cloud solution with broad functionalities and an impact on all corporate functions is often difficult or impractical. A cloud system for a particular functional area (such as research & development), for discrete events (like games or conventions) or for a specific geography may be wiser—with tailored services and safeguards to better meet data sovereignty, security or latency needs. This is also easier for organisational change management because cloud capabilities address core demands.

To meet more stringent demands for oversight and control, Ms Randery predicts that specialised but adaptable solutions that serve particular functions or geographies will grow. “Specialised is easier to outsource,” she notes. “It facilitates a greater level of migration and creates greater organisational resilience.”

But the push towards specialisation

demands different approaches based on, for example, specific risks or regulations.

In retail, for instance, the regulatory focus is on maintaining the privacy and confidentiality of customer data and compliance with the Payment Card Industry Data Security Standards (PCI DSS) to protect credit cardholder information.

PCI DSS compliance is also critical for financial services, as is adherence to the US Gramm-Leach-Bliley Act, which requires financial institutions to establish standards for protecting the security and confidentiality of their customers' non-public personal information.

In healthcare, the US federal Health Insurance Portability and Accountability Act (HIPAA) requires healthcare organisations to maintain the confidentiality of electronic health information that can be linked to an individual patient (also known as electronic protected health information, or ePHI). As Kristin Darby, chief information officer at Cancer Treatment Centers of America (CTCA), notes, HIPAA/ePHI compliance in the cloud is a particular challenge.

“Many specialised application vendors are simply forcing their existing desktop versions onto a cloud platform, without having ensured the integrity and interoperability of data, functionalities and workflows,” Ms Darby notes. The main barrier to greater cloud

adoption among healthcare companies today is the "shortage of cloud providers who can meet the industry's unique requirements around compliance and availability and can provide single tenancy at an affordable cost", she adds.

2. Systems integration and governance.

Today's cloud ecosystem is a mix of cloud types, multiple cloud providers, many cloud instances and specialised systems and applications native to individual departments. "We are concerned about application sprawl and loss of organisational resilience due to the ease of use and implementation of cloud-based solutions, especially when done without enterprise awareness," cautions Ms Darby.

The "sprawl" Ms Darby references, if unchecked, will pose a significant resilience risk to organisations and has pushed CTCA to add more process controls to contain this growth. As Ms Randery of Schneider Electric points out, "Data fragmentation is good from a risk perspective, but who's watching all that? When you have multiple cloud providers, how do they talk to each other?"

More-advanced cloud users are already

recognising, and many are addressing, the importance of oversight, connections and accountability. Respondents who say their organisations are ahead of competitors in organisational resilience are more likely to prioritise their efforts to strengthen internal processes and integrate new and legacy systems (see Figure 5).

3. Data and process re-engineering. Among the greatest challenges companies face after moving assets to the cloud is connecting existing data sets, business processes and workflows to the newly adopted technology.

First, executives must ensure that the data and systems they are moving are clean, organised and ready for migration. "How do you outsource a mess? What ... if you don't fully understand your own existing data and legacy systems?" Ms Randery of Schneider Electric asks.

More important, for greater resilience, proper alignment and flexing of the day-to-day workflow and business processes are critical to capture and monetise the efficiencies, productivity and increased resilience cloud computing promises. As Harsh

Figure 5. Where will your organisation prioritise its efforts to ensure organisational resilience over the next three years?

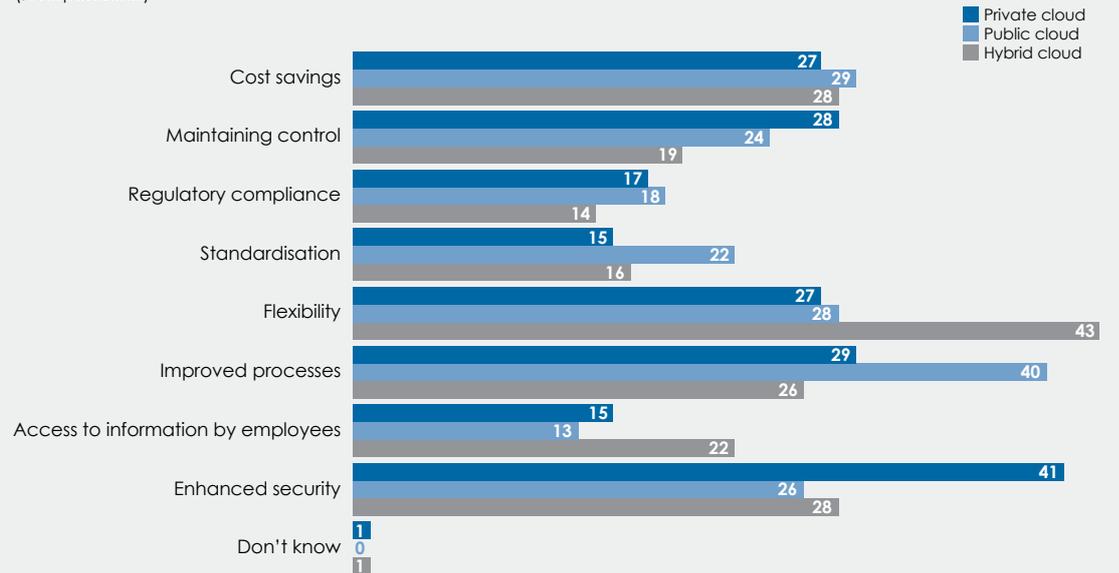
(% respondents)



Source: Economist Intelligence Unit, 2016.

Figure 6. What are the top two benefits of your cloud computing approach?

(% respondents)



Source: Economist Intelligence Unit, 2016.

Sinha, vice president, Engineering of money transfer company TransferWise, points out, “Companies need to re-architect to move to the cloud.” Often the heavy lifting required may prompt a company to keep legacy systems in house—or, sometimes, to shut them down altogether.

Indeed, lack of processes is a top challenge to cloud adoption for one-fifth of respondents in the EIU survey. To shore up resilience after cloud expansion, companies will need to work closely with partners to ensure that everyday processes seamlessly connect with the new cloud interface. Done well, the payoff is clear. Between 26% and 40% (see Figure 6) of EIU survey respondents say improved processes are a top benefit of their cloud use, perhaps attributable to the greater access, speed, agility and collaboration the cloud enables.

4. Ongoing service and maintenance. As with any new IT platform or service, moving to the cloud is not a one-and-done deal. Keeping systems updated, running and bug-free, and responding to user queries, feedback and service needs are perhaps more important

than the initial migration. “You have to make sure you have enough people doing the right things: patching systems, overseeing the physical security of IT assets, linking your organisation with that of the cloud provider,” says Mr Guinard of EVERYTHING.

This upkeep and customer service can be a significant challenge. But addressing this early can pay dividends. “Cloud can be a little bit impersonal,” remarks Ms Randery of Schneider Electric. “On-the-ground support for users is very important.” Ensuring the right level of service and support both in-house and through a cloud provider for both implementing cloud solutions and shoring up organisational resilience is critical.

5. People and skill sets realignment.

Successful adoption of any technology ultimately hinges on the human element. The right mix of skills, a smooth transition to new technology and a prompt embrace of a more agile and evolving process and culture by stakeholders will help companies reap the expected value from new cloud implementations.

“Technology is easier,” cautions Mr Sinha of

TransferWise. “The bigger resilience challenge is organisational. Companies need to retool their people for cloud computing. It requires significant change management.” But the extent of the challenge very much depends on an organisation’s culture.

“You need different people,” seconds Mr Guinard of EVERYTHING. System administrator skills were most valued before; now

developers who manifest agility and speed are in demand. Unfortunately but understandably, these skills are also valued by start-ups and are costly. Longer term, to build resilient cloud-based capabilities, companies will need to better understand the human needs of those who are implementing and maintaining their cloud-based strategy. ■

3

Conclusion: mindsets and partnerships for resilience

The rapid march into cloud computing has increased and will continue to increase the complexity and speed of change of IT ecosystems. In this often fragmented and always fluid environment, a different mindset—shifting focus from continuity to resilience—is needed to capture the efficiency, agility and economic gains promised by the cloud; anticipating or responding to negative disruptions will also be required.

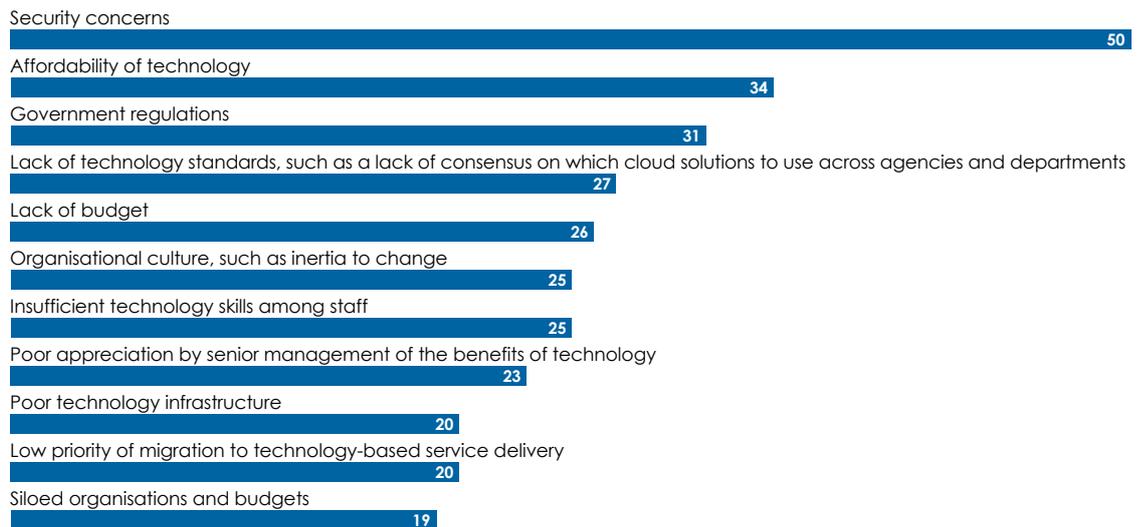
IT executives must rethink strategies, re-engineer operating models, retool talent and reinvent governance and decision-making. To do so, they will need to engage more stakeholders across an organisation. They will need to forge partnerships to better anticipate and address risks, to avoid disruption and to adapt to dynamic market, technology and regulatory environments. ■

Appendix: survey results

Percentages may not add to 100% owing to rounding or the ability of respondents to choose multiple responses.

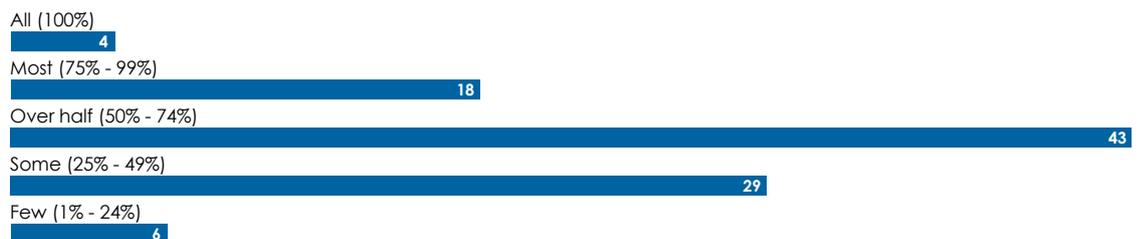
In your opinion, what will be the greatest barriers to broader technology adoption in your organisation over the next three years?

Please select the top three.
(% respondents)



What portion of your organisation's systems are cloud-based (public and private) today?

Select one.
(% respondents)



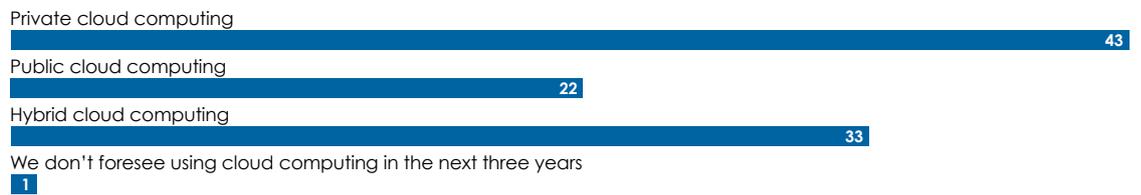
Which type(s) of cloud computing services does your organisation currently use?

Please select all that apply.
(% respondents)



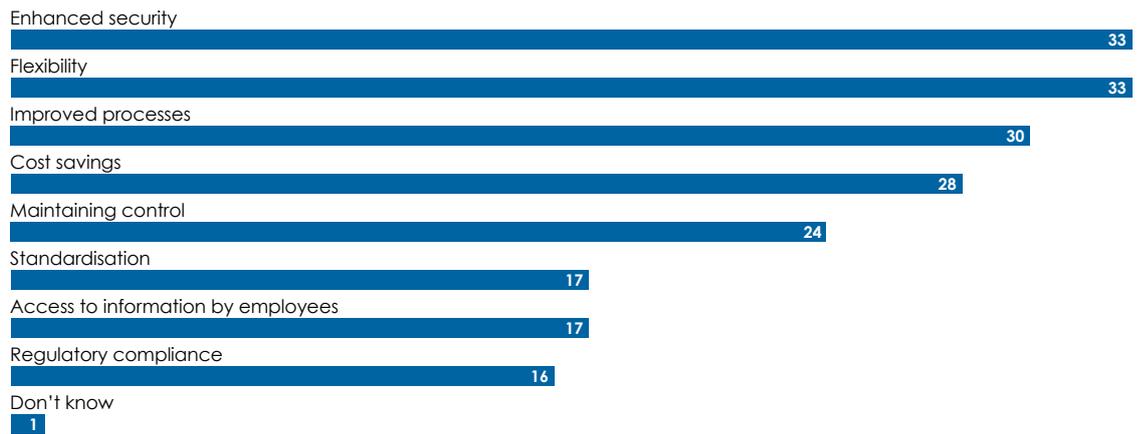
Over the next three years, what will be your primary approach to cloud computing?

Please select one.
(% respondents)



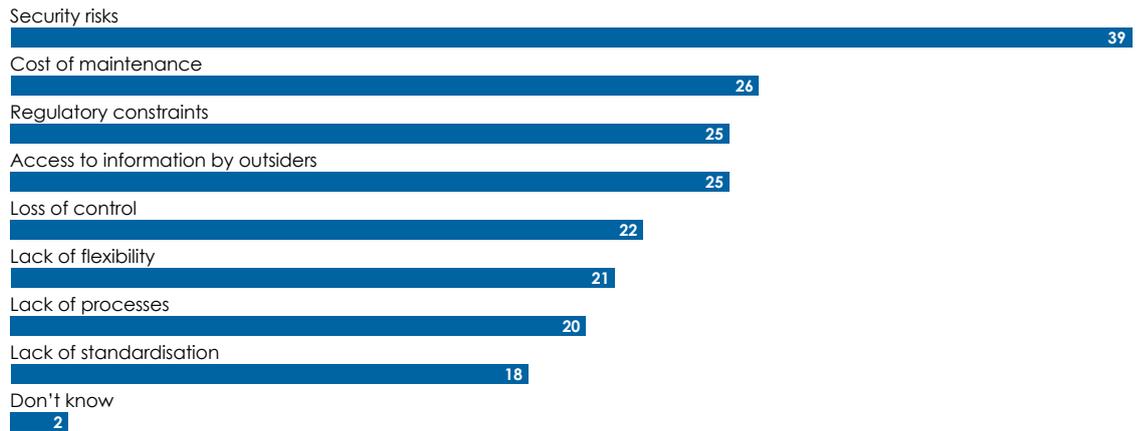
What are the top two benefits of your primary approach to cloud computing?

Please select two.
(% respondents)



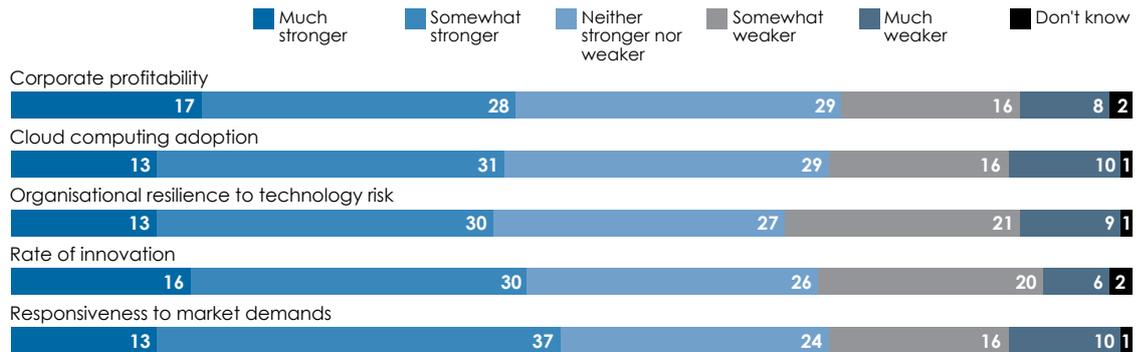
What are the top two challenges of your primary approach to cloud computing?

Please select two.
(% respondents)



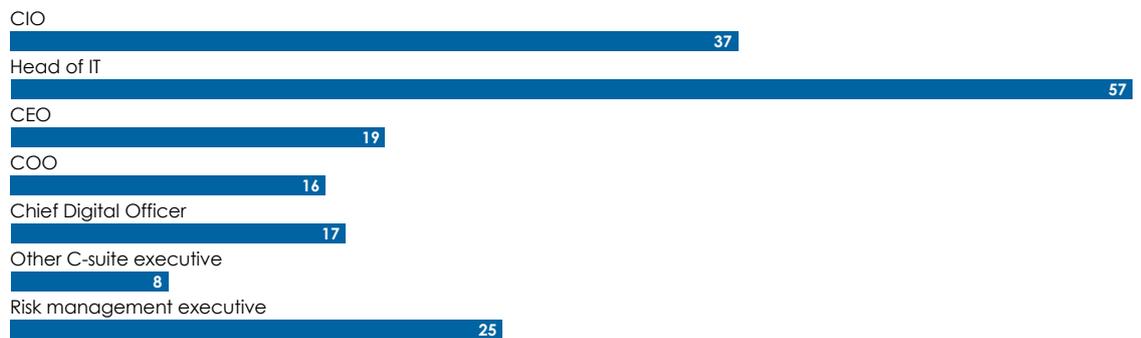
In your opinion, how does your company compare to its closest competitors in the following areas?

Rate on a scale of 1 to 5, where 1=Much stronger and 5=Much weaker.
(% respondents)



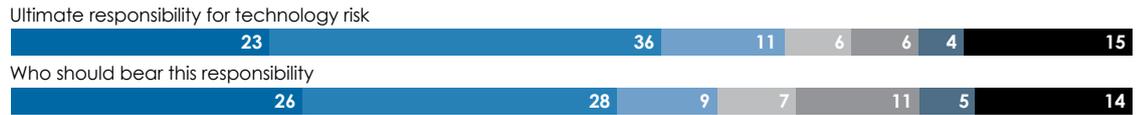
In your organisation, who is involved in identifying business continuity risks?

Select all that apply.
(% respondents)



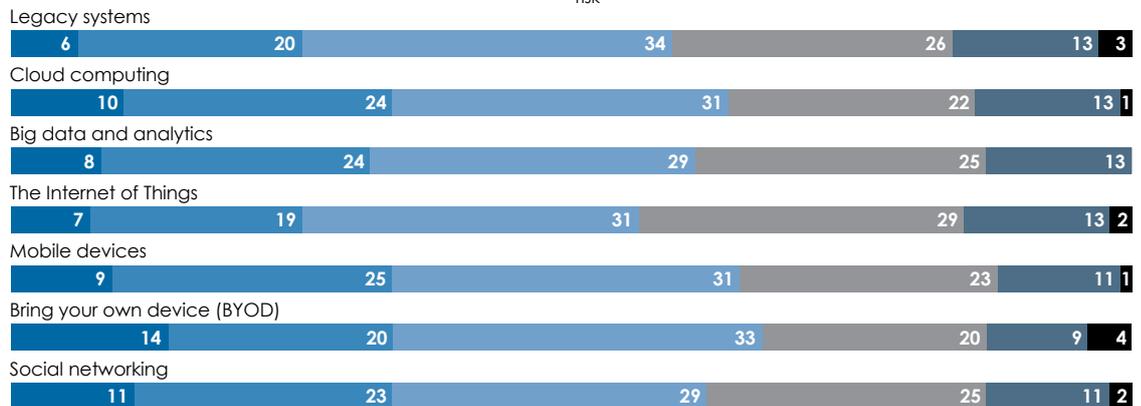
In your opinion, who within your organisation is ultimately responsible for managing technology risk? Who do you believe should be responsible?

Please select one in each column.
(% respondents)



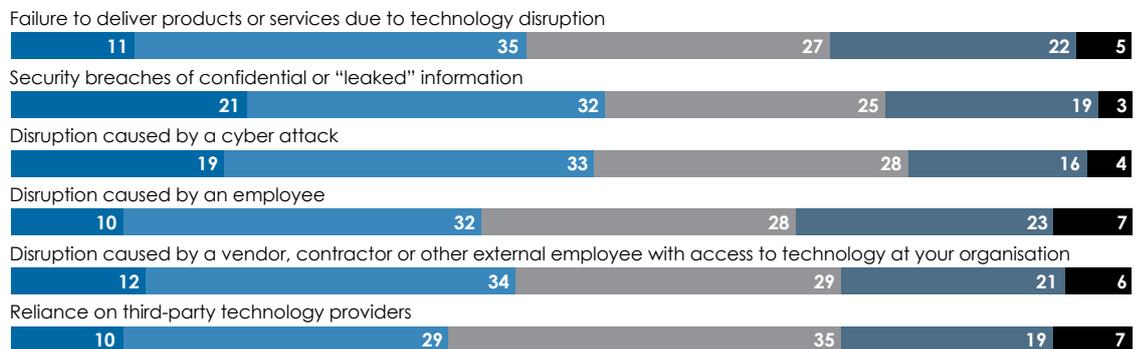
Which of the following uses of technology, in your opinion, pose the biggest risk to your organisation's business continuity over the next three years?

Please rate on a scale of 1 to 5, where 1=Major risk and 5= No risk.
(% respondents)



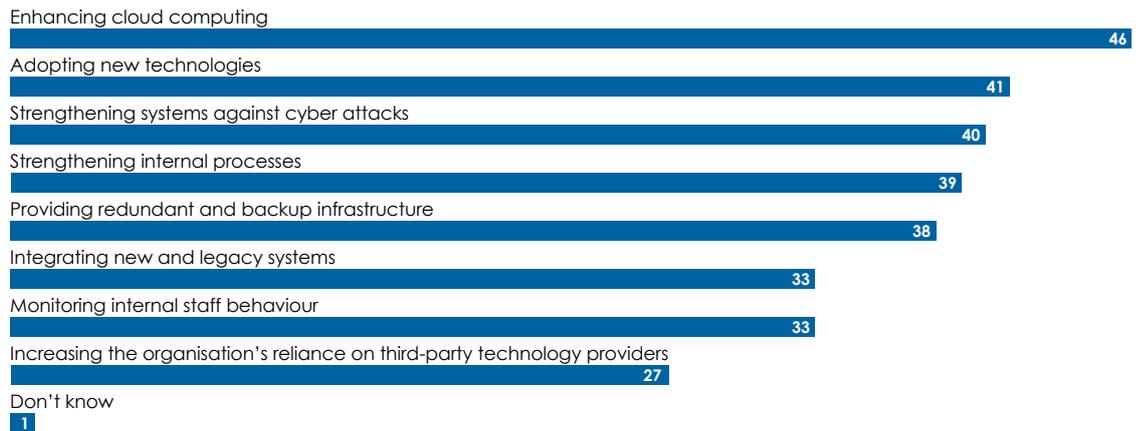
How concerned are you about the following risks to your company's reputation over the next three years?

Rate on a scale of 1 to 5, where 1=Extremely concerned and 5=Not at all concerned.
(% respondents)



Where will your organisation prioritise its efforts to ensure organisational resilience over the next three years?

Please select three.
(% respondents)



Please rate your level of agreement with the following statements:

Please select one in each row.
(% respondents)



What is your main functional role?

Select one.
(% respondents)



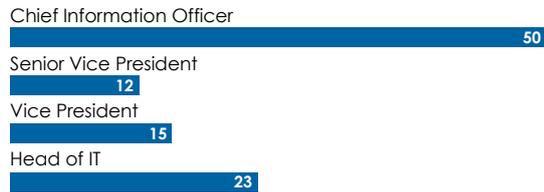
In which country are you personally located?

(% respondents)



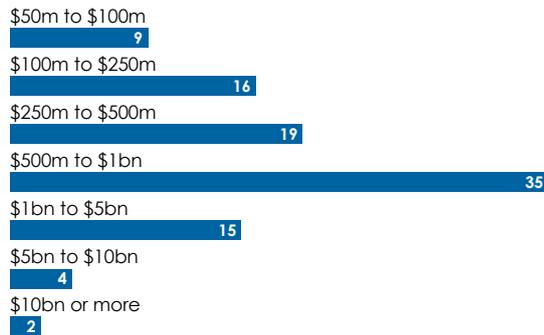
Which of the following best describes your title?

(% respondents)



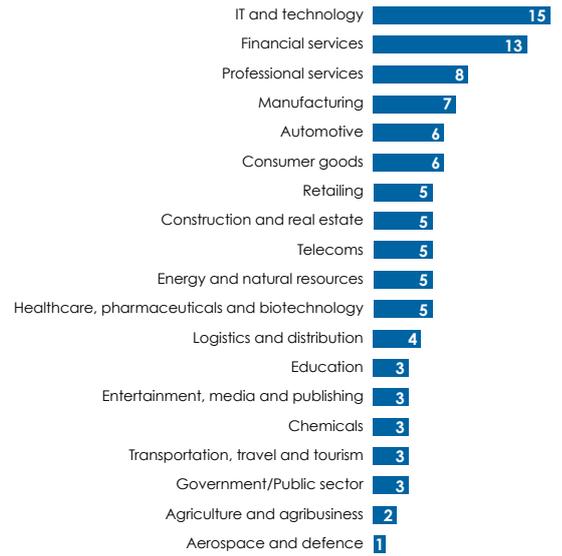
What are your organisation's global annual revenues in US dollars?

(% respondents)



What is your primary industry?

(% respondents)



Whilst every effort has been taken to verify the accuracy of this information, neither The Economist Intelligence Unit Ltd. nor the sponsor of this report can accept any responsibility or liability for reliance by any person on this report or any of the information, opinions or conclusions set out in the report.

London

20 Cabot Square
London
E14 4QW
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8476
E-mail: london@eiu.com

New York

750 Third Avenue
5th Floor
New York, NY 10017
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 0248
E-mail: newyork@eiu.com

Hong Kong

1301 Cityplaza Four
12 Taikoo Wan Road
Taikoo Shing
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
E-mail: hongkong@eiu.com

Geneva

Boulevard des
Tranchées 16
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
E-mail: geneva@eiu.com