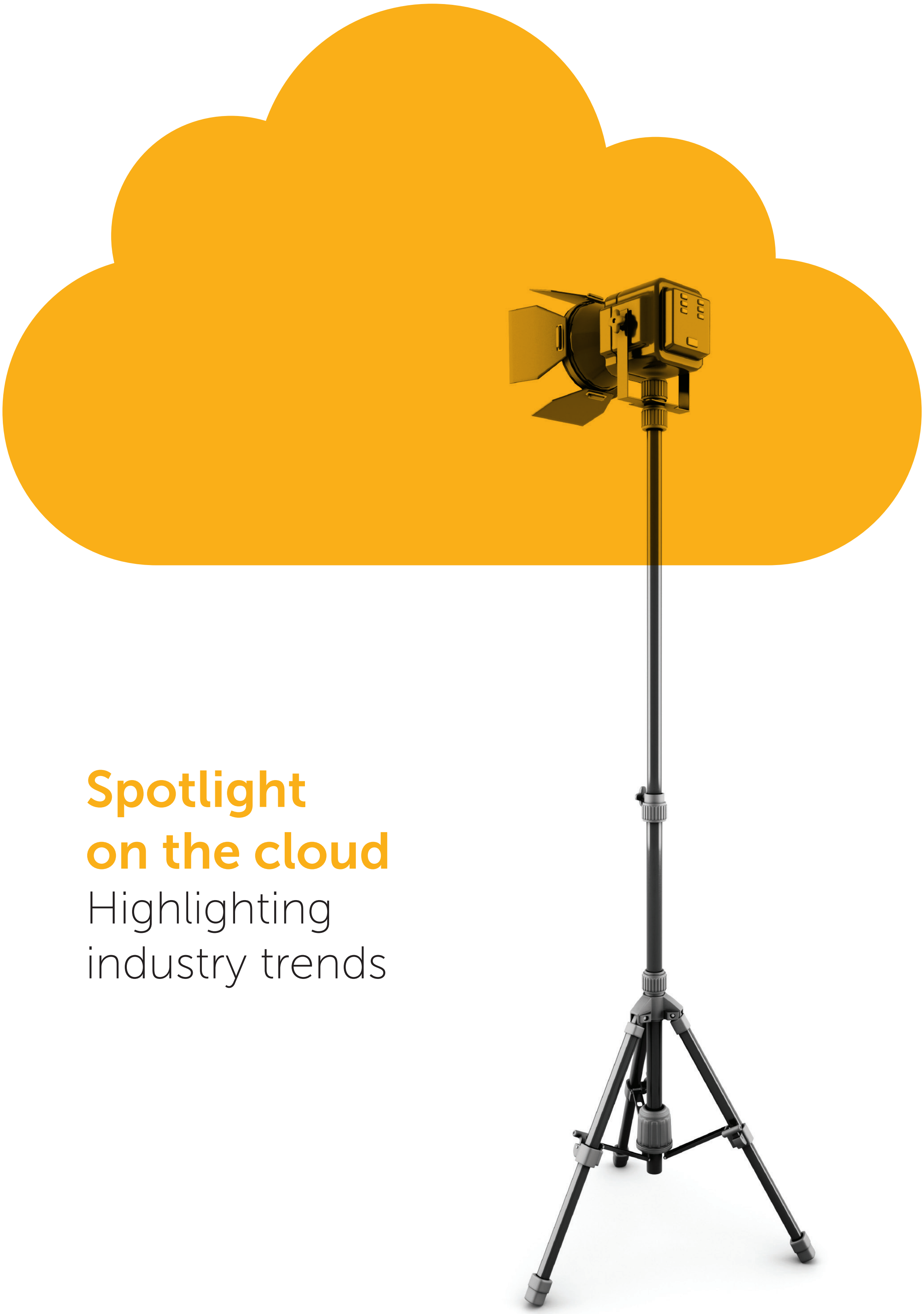
EVERSHEDS

THE LAWYER



Spotlight on the cloud

Highlighting industry trends

Spotlight on the cloud
Highlighting industry trends

By Charlotte Walker-Osborn, Global Head of Technology, Media & Telecoms, Eversheds LLP and Thomas Sturge, Head of Research, *The Lawyer*

Contents

Executive summary

Welcome to 'Spotlight on the cloud: Highlighting industry trends', a report produced by Eversheds LLP in collaboration with *The Lawyer*. Underpinned by detailed analysis of a global survey of 350 cloud providers, purchasers and industry advisors, and supplemented with interviews with major industry stakeholders, this report explores current and emerging trends in cloud computing adoption, contract negotiation and M&A.

A surprisingly large number of cloud sales deals break down at the contract negotiation stage. This is one of the key findings of our survey and is an issue that needs careful consideration by customers and providers of cloud solutions, not to mention advisors on these deals.

Just how many deals break down during negotiation? Some 27% of surveyed cloud customers have walked away from at least one deal once it got to contract negotiation, and a further 10% have nearly walked away from a deal at this stage. Furthermore, over half of cloud providers have lost or nearly lost a cloud deal during negotiations.

We believe this is an unnecessarily high figure given that customers and suppliers have typically reached agreement, at least in principle, before deals get to contract negotiation. Our view is that more engagement around difficult issues at the outset would reduce these figures significantly.

It is important to consider why deals break down at this juncture. The two most commonly mentioned reasons both relate to data residency. Over 30% of respondents have walked away from a cloud deal because they just don't feel comfortable that they know where their data is hosted. The same proportion have walked away from a deal because they know where the data resides but they don't like it.

In each case, early conversations around these points may have allowed a deal to be reached with a slightly different cloud solution and with the same vendor. Even if this wasn't the case, it is better to know if there is a mismatch of requirements and service early on to avoid wasted effort.

Of course, other factors cause cloud procurement deals to fall apart during negotiations. The other most common deal breakers cited include concerns over security breach reporting, insufficient visibility and responsibility for subcontracted elements of the service, concerns that the contract does not match the sales literature, and concerns that the supplier might change the service once the contract is signed. Again, engagement around these issues can often ensure the deal goes through.

Importantly, the above are all reasons why cloud customers think the deal collapsed. But ask cloud providers the same question and you get a very different answer. Indeed, cloud vendors pinpoint two factors above all others that trigger deal breakdown – price and, although harder to pinpoint, political, cultural and regulatory restrictions. There is a clear difference of opinion on this point.

We don't want to characterise the cloud industry as one beset with collapsed deals and misunderstanding and miscommunication between buyers and sellers of cloud. Indeed. Despite some instances of deals collapsing during negotiations, the general story around cloud is extremely positive. Indeed, Eversheds has helped its clients with, and therefore seen a great number of, "win win" deals struck between suppliers and customers.

Cloud adoption has surged in recent years. Cloud venture capital specialist Bessemer Venture Partners estimated that the global cloud market was worth US$56.6 billion in 2014, ten times the market size in 2008. Our survey data indicates this trend will continue – almost eight out of ten surveyed cloud purchasers expect to increase their level of cloud spend during the next 18 months. Only 1% forecast a decrease.

A constant message from the survey data is that it is imperative to consider the legal and related technical and commercial aspects at the outset of the process and, whether you are a supplier or a customer, ensure that both parties have the same understanding of the deal. This enables a smooth transition to the deal documentation.

It is clear that one of the key reasons that deals are failing at negotiation stage is because this is when many of the trickier issues (legal and related technical/commercial issues) become clear, including whether the parties are apart around these issues. Conversations around these points early on can avoid issues materialising way down the negotiating track and, frankly, wasted time and money on both sides.

By far the most important point to consider when heading into the negotiation room are terms relating to data and specifically data protection. Half of customers that aborted a cloud deal at contract negotiation stage did so because agreement could not be reached on acceptable data protection terms. We know that most cloud suppliers take issues of data protection and security very seriously, so a conversation around this area early on, we believe, would mean more successful deals are struck, even if the deal shape/solution changes slightly.

It is important that the service selected and/or configuration being considered allows compliance for the customer. Again, this should be considered on both sides early on to avoid wasted effort.

Data and security issues aside, our survey data reveals there are issues surrounding service level agreements, liability clauses and exit provisions that need to be considered carefully when negotiating cloud contracts. The winners in the supplier context take these very real customer concerns into account and do seek to ensure customers feel they have adequate coverage in these areas, in conjunction with offering a great service.

It is recognised by some that public cloud and certain hybrid services may necessarily not be able to allow any or as much flexibility in some of these areas. It is clear that early explanation by providers as to what is or is not included in their service offering is key.

If you have any questions about the findings, or would like to explore how Eversheds can assist your organisation, please feel free to contact me or indeed any of the individuals listed at the end of this report.

Charlotte Walker-Osborn
Global Head of Technology,
Media and Telecoms

T: +44 121 232 1220
M: +44 779 907 5756
charlottewalker-osborn@eversheds.com

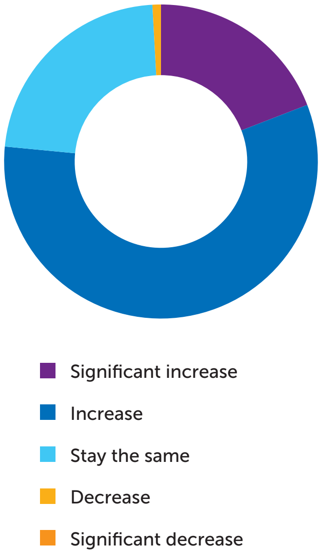
The state of cloud uptake – who, what and why?

Cloud spending on the rise

Pretty much every cloud computing market study arrives at the same conclusion – use of cloud has grown significantly in the last five years and adoption rates are showing no signs of decreasing. Vodafone’s Cloud Barometer 2015 estimates that 77% of enterprises used some sort of cloud at the end of 2014, a figure predicted to increase to 89% by the end of 2016. In terms of market size, cloud venture capital specialist Bessemer Venture Partners estimated the cloud computing market was US$56.6 billion in 2014, of which US$26 billion was spent on private cloud. This is a huge increase on the US$5.6 billion estimated market size in 2008.

Our survey data indicates that this growth will be maintained – 77% of surveyed purchasers of cloud expect to increase their level of cloud spend during the next 18 months while only 1% forecast a decrease. This is in stark contrast to the findings in “Canvassing the Cloud”, produced by Eversheds and PA Consulting Group in 2013, which predicted much slower uptake. This is a clear indication that cloud has become much more accepted in the last three years.

How do you expect your level of spend on purchasing cloud services to change in the next 18 months? (Purchasers)



What is driving this increase? Interestingly, customers and suppliers have differing views on how cloud benefits users. Some 31% of surveyed cloud providers believe scalability is the most important advantage cloud offers customers. This is double the number of suppliers that selected any other cloud business advantage as the most important reason for adoption.

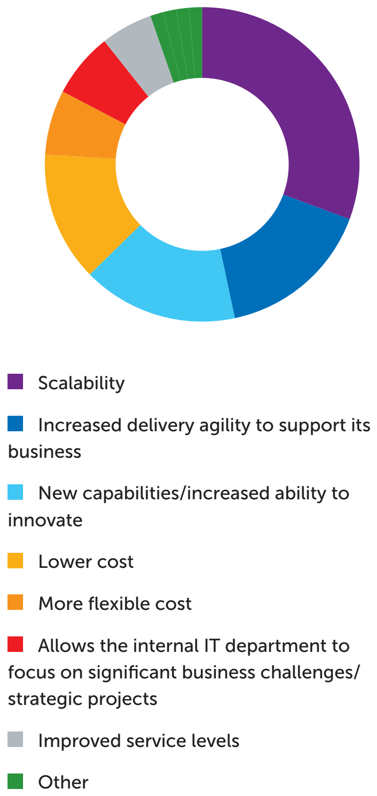
The main reasons for buying cloud are similar on both sides of the Atlantic. European cloud companies sited scalability as the primary reason for uptake, followed by lower cost and increased delivery agility. US cloud companies also mentioned scalability as the number one reason for uptake, followed by an improved ability to innovate and then increased delivery agility.

In contrast, purchasers highlight increased delivery agility to support their business and that cloud allows internal IT departments to focus on significant business challenges/ strategic projects as the two most important benefits.

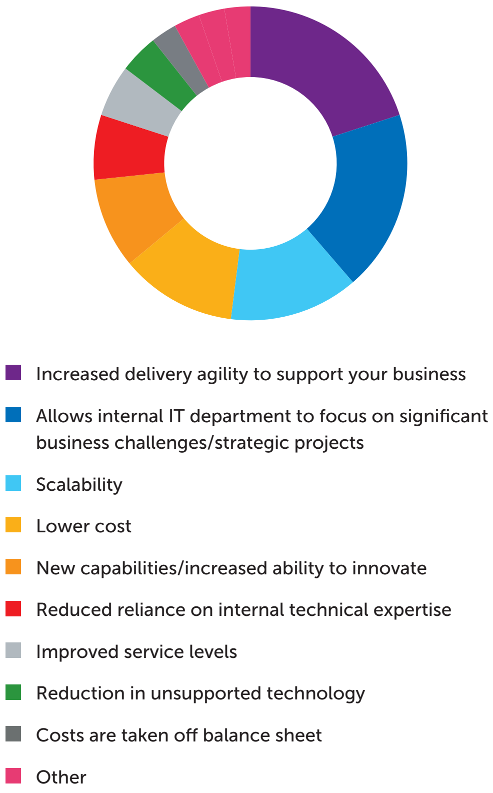
One might consider that scalability and flexibility go hand in hand. But there is a subtle difference. The survey data suggests customers see cloud as an essential part of their IT infrastructure because it enables them to swiftly and effectively serve the changing needs of their own customers, rather than because it enables them to cope with sizeable changes in demand, unless there is particular sector or functionality rationale.

Of course, the importance of scalability depends on the industry and the function that is being put onto cloud. Scalability is clearly very important for sectors such as retail to help cope with times of huge demand, such as Black Friday and seasonal holidays. But the retail sector is unusual in this respect and many other sectors have a flat or moderately increasing need for cloud capacity, barring any unusual event such as a major acquisition, disposal

What are the main benefits your business offers to customers adopting its cloud services? (Providers)



What are the main benefits of adopting cloud services for your business? (Purchasers)



or a product launch. For most sectors, it is therefore understandable that scalability is not the main factor driving customer adoption.

Why is this important? The survey data reveals a degree of mismatch between the key benefits some suppliers are marketing and why customers wish to buy. In practice, many customer expectations outlined in the diagram above are offered by many cloud providers. But it may make sense for vendors to consider their sales messaging so that the other benefits are marketed more fully.

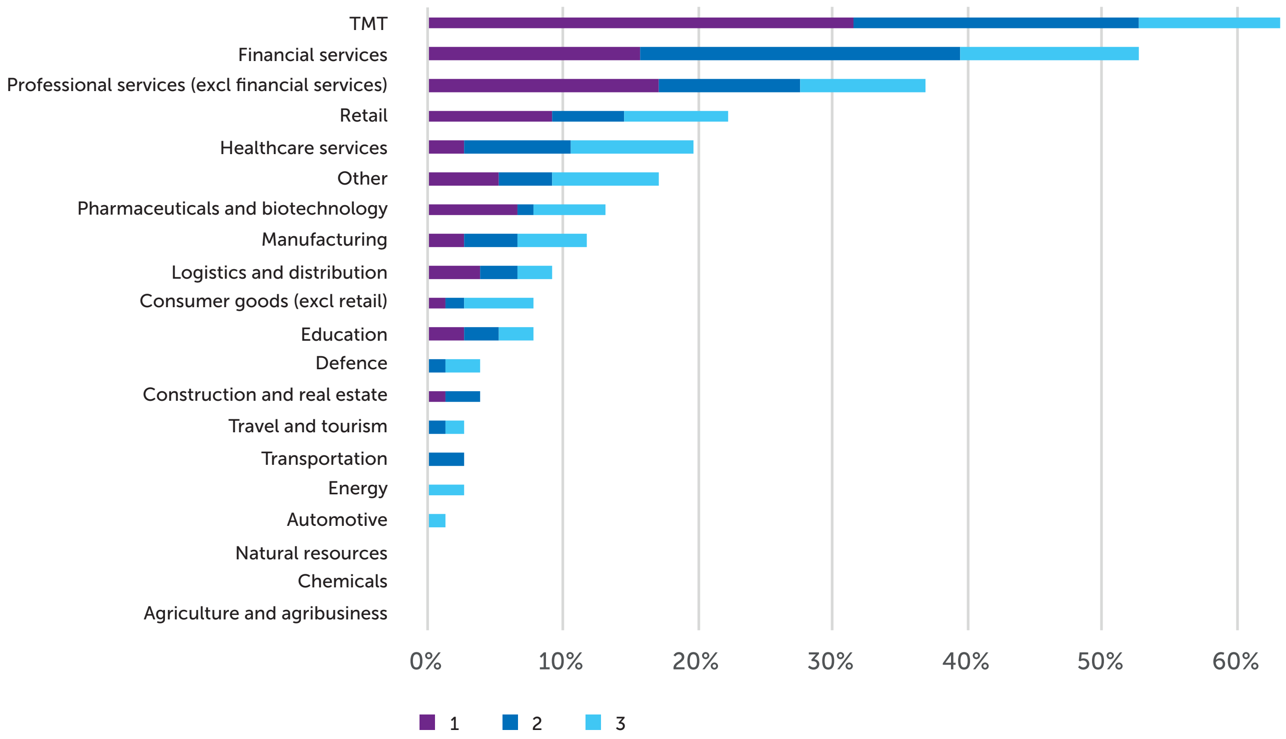
Cloud uptake has been slower in Asia. There are two primary reasons for this. First, although there are some obvious exceptions, culturally, companies are less comfortable, it seems, with outsourcing in general, including cloud. In addition, the regulatory environment for cloud computing is not only less clear in Asia than Europe and the US, but is also subject to more frequent changes.

"Asian companies' reticence to adopt cloud is partly cultural and a reluctance to lose control amid worries about confidentiality, data security and IT security," explained Nigel Stamp, Partner, Head of TMT in Asia, at Eversheds. "But it's also partly due to the regulatory environment. You've got so many different jurisdictions in Asia and the regulatory environments in these jurisdictions are less developed than in the US, UK and Europe, particularly when we get to cloud."

Future adopters

Three industries are currently at the forefront of adopting cloud solutions according to surveyed solution providers. Some 32% of respondents situated around the world are currently experiencing greatest demand from the TMT sector (who are likely most comfortable with the concept of cloud), while 17% are seeing greatest demand from professional services and 16% from financial services. Interestingly, our survey data also shows that cloud uptake is fastest in different industries in Europe versus North America. Surveyed European cloud companies are currently experiencing greatest demand from the TMT sector, followed by financial services and then professional services. Surveyed US cloud companies are also seeing most demand from the TMT sector, but following this are experiencing most demand from pharmaceuticals and

From which industries are you experiencing greatest demand for cloud services? (Providers)



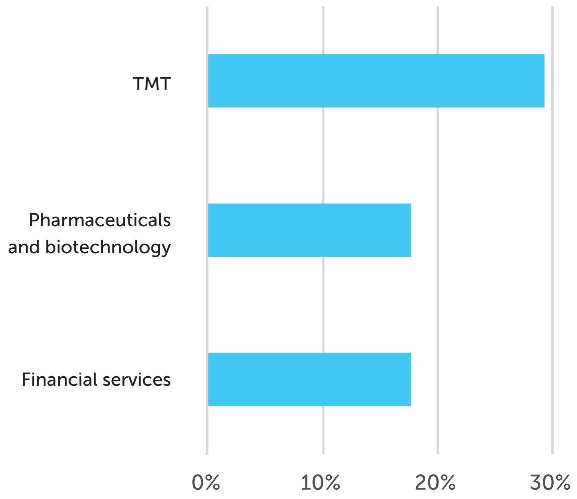
Note: - Respondents citing 'other' primarily saw greatest demand from central government and the legal services industry
- Respondents were asked to select their top three industries, with one being the most common

biotechnology companies.

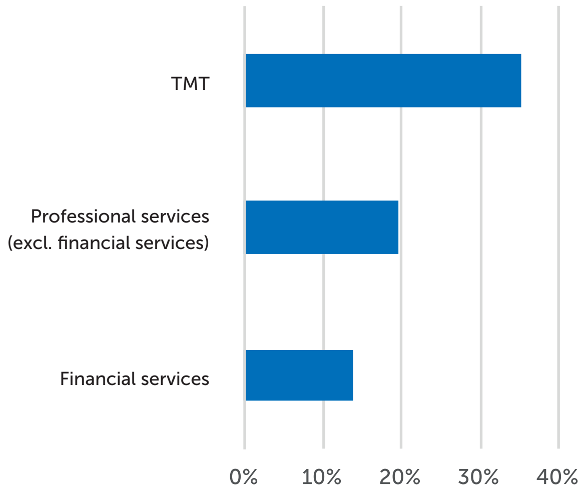
It is notable that cloud vendors consider the financial services sector to be the third most active purchaser, or indeed the second most active when providers' top three most active sectors for cloud purchasing are aggregated.

Adoption in this sector has traditionally been slower given the high level of regulation financial services companies are subject to regarding personal data and outsourcing. However, as explained in the box below, recent guidance

From which industries are you experiencing greatest demand for cloud services? (US cloud providers - top three sectors only)



From which industries are you experiencing greatest demand for cloud services? (European cloud providers - top three sectors only)



Focus on financial services – regulatory guidance aids adoption

Many large financial services companies operate in multiple jurisdictions, meaning they are subject to a variety of regulatory frameworks. These regulations will often stipulate what due diligence should be undertaken on third party outsource and IT providers, how contracting should be undertaken, and how that third party should be managed and monitored. There are also likely to be separate requirements relating to data privacy, and in particular knowing where data is stored at any point in time.

On top of this, regulations that relate to the use of third party outsource or IT providers are often unclear when they are applied to cloud computing transactions. This is because they were designed for more general business process or traditional IT outsourcing and were not written with the cloud specifically in mind.

A good example (from the UK) is the requirement for a financial institution (and regulator) to have effective access to data and the service provider's premises*. This is commonly referred to as a right of "audit" and does not translate easily to cloud services provided from multi-tenanted data centres. This has resulted in some financial services companies being reluctant to adopt cloud solutions due to concerns that they will not be compliant with the regulatory framework within which they operate.

Mark Bennett, Executive Director, Head of IT Legal, Legal and Compliance at Nomura International, explains the regulatory scenario many financial institutions face. "We not only have to comply with a maturing Asian regulatory regime, where literally every day another nation puts through new regulatory requirements, but also the regulatory requirements in the US and the EU, which are more established but more complex," he said. "On top of all this we recently have the loss of safe harbor in more mature regions. It is a major challenge and our compliance people are very busy."

This is not only an issue for potential customers. Some suppliers have struggled to design solutions for this industry when the regulatory requirements are unclear. Other vendors have cleverly used this as a strong selling point if they believe their solution overcomes and fulfils regulatory hurdles.

Providers have certainly become more attuned to regulatory demands and customers' concerns over audit and due diligence, regardless of whether they are regulated or not.

"We appreciate that it's important for customers to choose a cloud solution which satisfies regulatory requirements," comments Helen Kelisky, VP Cloud (UK & Ireland) at IBM. "Our teams work with independent auditors and third-party organisations to meet the industry's most stringent guidelines for reporting, security and compliance. These include certification for ISO 20001 security standards, ISO 20018 controls for personal data, and an attestation of compliance for the Payment Cards Industry (PCI-DSS). We also work closely with clients in regulated industries to provide them with the evidence they need to demonstrate that they have undertaken appropriate due diligence of our services before moving workloads to the cloud."

Additionally, some countries are taking steps to help financial services companies navigate these regulatory challenges. For example, in November 2015 the UK Financial Conduct Authority (FCA) published proposed guidance for firms outsourcing to the cloud. It is the first step in a process that, following consultation, will lead to a final report and set of proposals.

The FCA's initial guidance stated they "see no fundamental reason why cloud services (including public cloud services) cannot be implemented, with appropriate consideration" while also complying with their rules and regulations. This guidance also included a check list of issues that need to be discussed when considering outsourcing to the cloud.

This guidance has been warmly received by the industry and might partly explain why financial services companies are currently amongst the most active purchasers of cloud solutions. "The FCA's document that attempted to itemise high level concerns to the industry was very impressive and the first time I had ever seen anything like this," explained Bennett. "It wasn't fully exhaustive but went a long way in setting the material issues that both cloud providers and financial institutions need to consider and discuss when negotiating."

Yet despite this improvement in the regulatory landscape, there are still large areas of uncertainty or hurdles to work through, meaning adoption will likely

* FCA Handbook 8.1.8(9); PRA Rulebook Outsourcing Rule 2.6(9); Solvency II article 38.1(b)-(c)

still be slow-paced. "Even though the FCA has stated they have no objection to cloud, adoption will be fairly slow and cautious," explained Simon Gamlin, Partner, International IT Group and International Outsourcing Group Lead at Eversheds. "They have said cloud services must be procured within the same regulatory framework as other outsourcing arrangements, and because that isn't prescriptive at all, it is very difficult for firms to get comfortable that they are doing what is required from a regulatory perspective when procuring cloud services. The regulation has general principles that were not written with cloud in mind. Customers are still not sure what protections are essential to have in the contract to meet these regulatory requirements. So we are in a bit of a transition period."

It is clear that the numerous benefits mean many financial services companies are grappling with their regulatory requirements in order to embrace cloud. Vendors who demonstrate that their solutions are compliant in their sales messaging, technical solution and contract documentation have a competitive advantage and will save immense time when contracting with their customers.

Still some concerns around public cloud

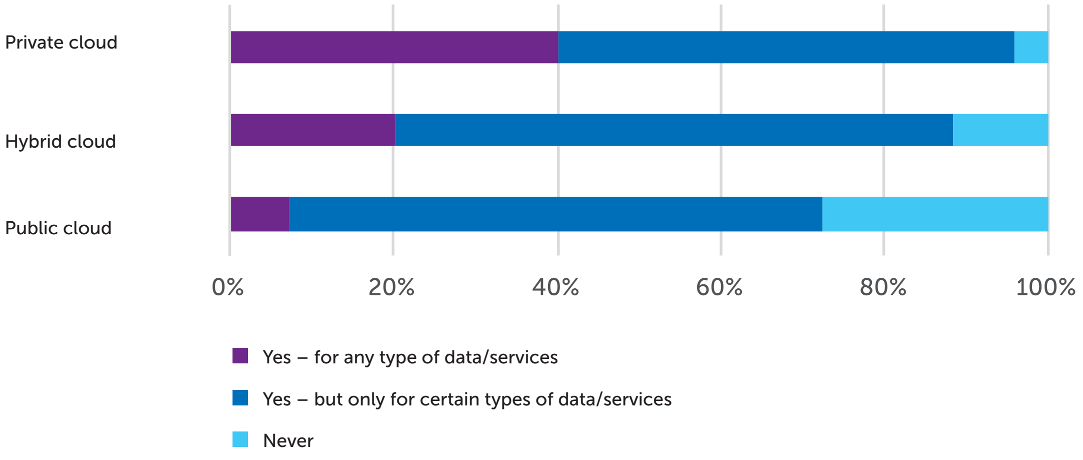
Although cloud demand is generally increasing, our survey data reveals there are still widespread hesitancies around adopting public cloud outside the US. Some 28% of surveyed cloud purchasers stated they will never adopt public cloud, while only 7% stated they would adopt public cloud for any/all types of data or services. In contrast, private cloud is viewed as a much safer option – only 4% of surveyed purchasers will never adopt private cloud and 40% are willing to adopt private cloud for any function.

It is important to note that the degree of reticence to adopt public cloud varies by region – some 42% of surveyed North American cloud providers stated their clients typically prefer public cloud. In contrast only 23% of European cloud vendors said their customers typically prefer public cloud.

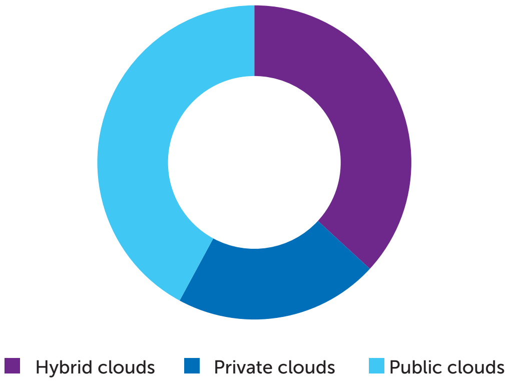
The reluctance to invest in public cloud is primarily driven by concerns relating to security and personal data. Interestingly, it is clear that not all purchasers are aware that many hybrid solutions are underpinned by some form of public cloud. Of course, many public cloud vendors, including all of the leading players, are likely to disagree with this perception and argue that significant investment allows them to lock down their infrastructure, platforms and services. The survey data reveals there is less of a concern for certain types of data in the US. In addition, some of the leading players (for example AWS) actively allow penetration testing by its customers within agreed boundaries.

Putting the debate about public clouds aside, the survey data also reveals some interesting trends about the types of cloud services that are in high demand. Customer-facing websites/portals, established SaaS applications and email have already been adopted most widely. Specific cloud services that look set to be in high demand in the next 18

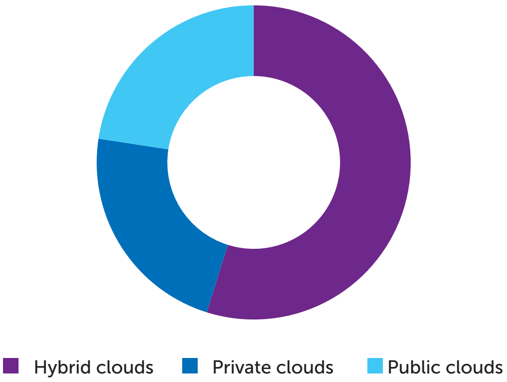
Would your organisation adopt the following types of cloud for use in its business? (Purchasers)



What are your clients' preferences regarding the type of cloud services procured? (Providers - North America)



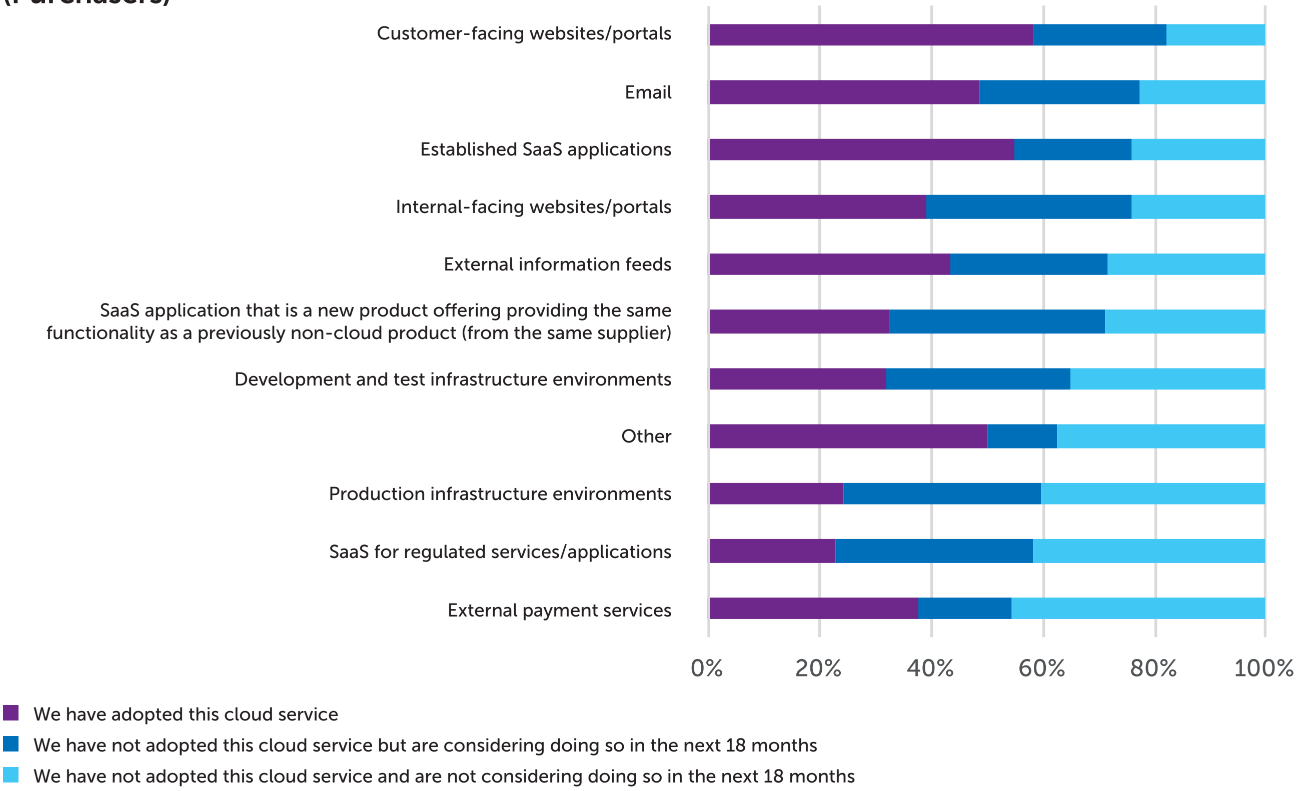
What are your clients' preferences regarding the type of cloud services procured? (Providers - Europe)



months include internal-facing websites/portals, production infrastructure environments and SaaS for regulated services/applications.

It is worth noting that customers are often pulled into adopting cloud for certain functions and services because their incumbent and/or preferred suppliers migrate them onto a cloud solution that has exactly the same functionality as their existing solution. In addition, the low uptake of cloud for functions such as external payment services is likely due to perceptions that the cloud is vulnerable to security breaches. Again, vendors who are able to alleviate these concerns to a sufficient degree are best placed to gain market share.

Which of the following cloud services have you adopted or are you considering adopting? (Purchasers)



Negotiating cloud contracts – still not a done deal

The final hurdle, but still a major one
The customer has made a business case to invest in cloud, the budget is approved, a cloud provider selected and extensive discussions have been undertaken with that vendor's sales team. Then the contract arrives. You might think the deal is almost done at this juncture. But our survey data suggests otherwise. Some 27% of surveyed cloud purchasers have walked away from at least one deal once it got to the contract negotiation stage. A further 10% have nearly walked away from a deal at this stage.

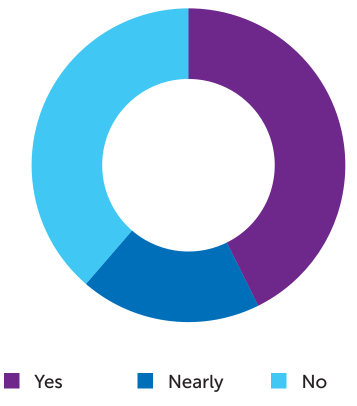
Cloud providers also realise this is an issue – 57% of surveyed cloud providers have lost or nearly lost deals at the contract negotiation stage.

Why is this? After all, one might expect ironing out the contract details is a formality if the agreement has already been made in principle between the purchaser and the provider's sales team.

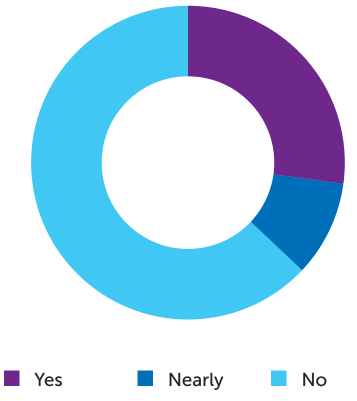
Mark Bennett, Executive Director, Head of IT Legal, Legal and Compliance at Nomura International, believes this occurs because many purchasers are not experienced cloud customers. "Often deals break down at negotiation, not because the provider is being unreasonable, although sometimes they might be, but often due to the unpreparedness of the customer," he said. "Customers often think they know what they want but often have no idea what they want. The sales brochure might look great but customers often haven't thought about how they integrate it and how it actually works in detail, so when they look at the actual granular level of the deal it becomes apparent that they were not ever ready for it. There was often never a deal to be done."

Certain factors cause deals to break down more frequently in certain regions. For example, in the Gulf region deals are more likely to not get fully off the ground or collapse than in other regions as there are still hesitations

Have any potential clients/actual customers ever walked away or almost walked away from a cloud deal which was part way through negotiations? (Providers)



Have you ever walked away from a cloud deal which was part way through negotiations? (Purchasers)



around adoption, both by government and companies. "Consumption of cloud services is still under consideration in the Gulf region," explained Ashraf Abdelwahab, Director of Corporate Affairs, Gulf & Egypt at Microsoft. "From a regulatory point of view, there is still a lot of work to be done to get confidence in cloud services. For example, data classification policy, data protection law and cybercrime law, are basic building blocks in the data management space that need to be in place to ensure safe cloud consumption."

The statistics above raise important messages for both cloud providers and purchasers. For providers, the relatively high number of customers who drop out at the contract negotiation stage could mean that the terms and conditions are too stringent and/or do not match the sales messaging. A more flexible approach might result in greater business.

However, what is even more apparent is that it becomes obvious the solution offered sometimes doesn't match the customer's requirements only when detailed legal discussions take place and a close look is taken at the service. On other occasions it becomes apparent that the solution is relevant but the purchaser needs to layer tools or services on top or take a differently located version of the service offering. Sometimes customers just need more information in order to satisfy internal due diligence and/or regulatory requirements.

Some vendors should therefore invest more time educating potential customers at the outset of discussions in order to be able to push the right service offering early on and to avoid aborting later on. After all, there is no point wasting sales peoples' time if the complete deal and contract is not right for the customer. Customers will welcome this.
For purchasers, these statistics show that it is worth thinking in detail about what type of cloud solution is appropriate for the business' requirements at the beginning of engaging with providers and requesting sight of the relevant contractual terms early on.

Having worked on numerous cloud deals over the years, we have seen some vendors, particularly in the public cloud space, taking the right amount of time early on in the deal to explain how the legal terms interact with and relate to the service being offered so that it is clear which terms are non-negotiable or have limited ability to be negotiated. In this way, at least the customer is clear and, if the customer has material issues with any of the terms, these can be faced together as the deal is being looked at. So, in summary, deals are often most successful when both parties get their differences out on the table early on as it enables any obstacles to be overcome swiftly.

Deals can hinge on data residency

What are the trigger points that cause cloud deals to break down at the negotiation stage? Our survey data indicates that the most important factor concerns where data is hosted, passes, or flows to and from. There are two primary issues. First, is that the purchaser does not always know where the data flows are, despite this information being requested – 31% of survey respondents have walked away from a cloud deal because they are in the dark about where data (and particularly personal data) is hosted. The same proportion have walked away from a deal because they are not comfortable with where the data resides or is accessed from once they know.

Cloud purchasers are anxious about where their data is hosted for two reasons. The first is regulatory. Data protection and privacy regulation differs by country, but most countries require companies to know where their personal (and at times non-personal) data is hosted, being processed and by whom. Companies operating in the EEA can also not transfer personal data outside the EEA unless certain safeguards are in place. This stance is being replicated in some countries outside the EEA too.

While most cloud providers are aware of data protection legislation, the degree to which it is addressed adequately in the contractual terms varies widely. It is therefore always worthwhile for purchasers to seek legal guidance to ensure they are contracting in a way that is compliant with data protection legislation. Conscientious providers will spend time understanding data flows and regulatory requirements and will ensure that this is converted into the contractual process and final contract. Vendors who are clear about how they allow compliance are much more likely to secure increased business, not to mention create good PR.

Of course, the degree of flexibility and fine-tuning of data security processes very much depends on the type of cloud. Suppliers will naturally be more flexible and accommodating on data security processes when it comes to private or even hybrid cloud solutions than public clouds. That said, many public cloud providers also offer a range of options around data security. This is not widely known and customers should be aware that they can create bespoke security controls for public clouds in certain circumstances.

The key is for customers to choose, with the assistance of suppliers, the right solution to meet any regulatory demands. This includes their appetite for risk and consequently the level of security and approach to data residency. Unfortunately, sometimes the solution is selected almost in spite of these factors. This wastes time and can hamper deals significantly.

US PATRIOT Act – spooking adopters?

Cloud purchasers are also nervous about data residency because, in certain jurisdictions, government authorities have the right to access personal data if it is hosted in their jurisdiction, or in some cases even outside their jurisdiction, if it is held by a company registered in their jurisdiction.

Rightly or wrongly, there is a strong perception that the US PATRIOT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act means US government and law enforcement authorities can access personal data hosted in the US.

The survey data indicates this is an important concern for cloud purchasers – 17% of surveyed purchasers that walked away from a deal at the negotiating stage did so due to concerns that company data may have to be given to government bodies due to local country legislation the cloud provider was subject to.

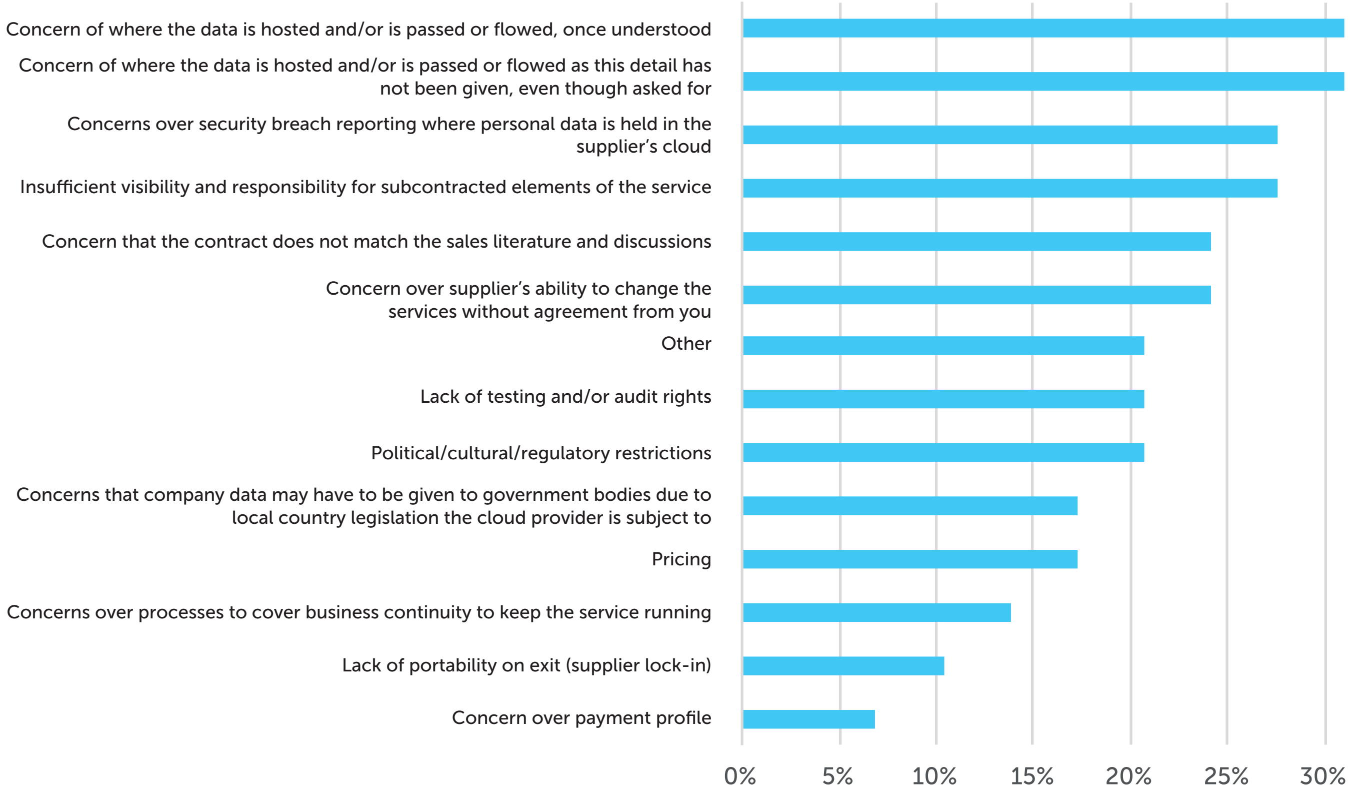
“These concerns have increased significantly over recent months,” confirms Paula Barrett, Partner and Global Head of Privacy and Information Law at Eversheds. “This was a contributing factor in the European Court of Justice decision which rendered the Safe Harbor framework for protecting personal data transferred to US from the EU as invalid.”

The ruling also continues to cast a shadow over alternative and replacement transfer mechanisms. Whilst many are exploring or have already put in place “EU” cloud solutions, there is more to this than simply the physical location of the server to be considered.

Whilst certainly not unique to the US, government access rights run counter to and fuel prevailing views in other countries. A clear example of this is Germany, where the data protection authorities encourage potential cloud customers to be very cautious about where data resides and who can access it.

“The big issue is data residency and the rights of seizure that the American Government might have on your provider,” confirms Alastair McAulay, Director of Disruptive IT, PA Consulting Group. “That is really spooking a lot of people now. For example, it caused one of the leading cloud providers to subcontract a cloud service to a German provider. You will buy through the lead provider but it won’t be provided by them. We did a job recently with a customer in the Middle East who was really worried that cloud data held in the US could be viewed by the government. This caused them to review their contract.”

What were the reasons for walking away from the deal? (Purchasers)



Lack of security breach reporting a potential deal breaker
The joint second most common reasons for cloud deals breaking down, according to purchasers, are concerns over inadequate security breach reporting where personal data is held in the supplier's cloud. Some 28% of surveyed purchasers of cloud solutions said they have walked away from at least one cloud deal because of this issue. Purchasers have strong requirements for security breach reporting for two reasons. Firstly, for the majority, there are certain regulations obliging security breach reporting when personal data is involved. The box on page 16 outlines what these regulations are and how they are changing. Secondly, regulation aside, purchasers are increasingly concerned about security breaches in light of high profile hacks at companies such as Talk Talk and Ashley Madison, so want to be kept informed of potential breaches. Eversheds is regularly helping both suppliers and customers deal with how to prepare for and respond to security breaches, as well as helping them if and when a breach occurs.

The changing regulatory landscape for security breaches and reporting

In many jurisdictions, organisations dealing with certain types of data are required to report if a security breach occurs. For example, in the UK, organisations are legally required to inform the Information Commissioner's Office (ICO) of data security breaches within 24 hours if they are a service provider covered under Privacy and Communications Regulations. There are also industry-specific reporting requirements for organisations that are, for example, regulated by the FCA. Even organisations that are not legally required to report a breach are expected to do so if the breach is serious and personal data has been compromised.

However, security breach regulation not only varies in different regions, with strong breach requirements in the US and a mixture across Europe, it is also currently undergoing significant change. New data privacy legislation (the General Data Protection Regulation or "GDPR") is expected to come into force in 2018 across the EU that will mandate relevant organisations to report breaches to the relevant data protection authority within 72 hours and in some cases to the individuals as well. With fines for non-compliance also set to increase significantly, as well as exposure to damages claims, the GDPR will raise the stakes for both cloud customers and providers in relation to both data security and security breach reporting where personal data is involved.

Another important aspect of the GDPR is that cloud providers will have direct responsibilities and liability for the appropriateness of data security and notification of breaches to the relevant data controller more generally when personal data is involved. Currently, cloud customers bear this responsibility in most EU countries and cloud providers face little or no statutory responsibility or direct liability to affected individuals.

Experience in the US and this forthcoming regulatory EU change have already triggered some cloud providers to review the language related to security and security breaches in their contracts.

"There are some issues in the language we are seeing," confirmed Paula Barrett, Partner and Global Head of Privacy at Eversheds. "We are seeing wording around security breach notification, but there are often questions about whether the breach notification is limited to when there is an actual loss of data, which is narrower than the current and proposed legislation requires. So you need to look quite closely at the breach reporting commitment to verify what the scope of it is, what is going to be reported, when are they going to report, how much cooperation will they provide in relation to breach response and who picks up the cost and potential liability."

These qualifications are usually driven by cloud providers' risk limitation. It is very risky for suppliers to provide generic breach reporting commitments because it involves significant time, effort and cost. Moreover, there are some very real operational issues associated with identifying that a breach has actually occurred, as well as limiting liability if it does.

The GDPR will most likely drive much more detailed due diligence by cloud providers into what data their customers are planning to process using their services, what they plan to do with it, and more specific statements on security standards and responsibilities. Many providers are already seeking indemnities for potential liability from their customers, making the data debate even more challenging.

Subcontracting risk of equal importance
Some 28% of surveyed cloud purchasers have walked away from a cloud deal due to insufficient visibility on, and responsibility for, subcontracted elements of the service. This is the same proportion that aborted a cloud deal due to concerns relating to security breach reporting.

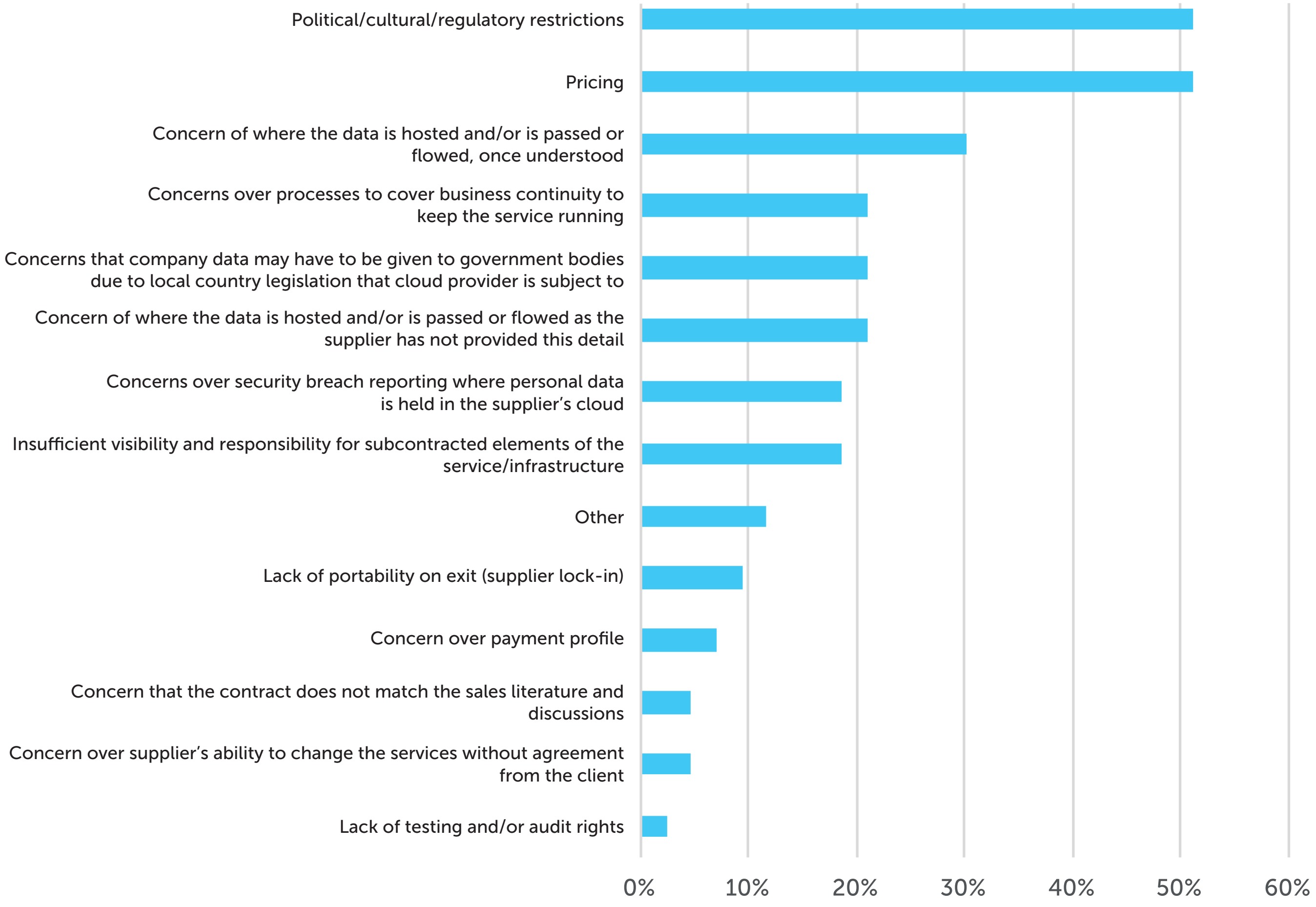
There are regulatory reasons, alongside sensible procurement practices, as to why customers need or want to have visibility of subcontracted aspects of cloud. Vendors who are very clear at the outset about who their subcontractors are and how they might change certainly help this area of the negotiations go much quicker.

In Eversheds' experience, cloud customers may become nervous in relation to potential changes to subcontractors once a contract has been signed. One way of remedying this, which we have seen at least a couple of vendors deftly apply, is to allow customers to sit in their user group(s) so that they can influence roadmap development. This also potentially enables vendors to at least talk to customers about their product development and subcontracting roadmap. Giving customers time to absorb this gets them comfortable or, if needed, provides time to migrate to a new provider.

Cloud providers don't understand why deals collapse
Our survey data reveals a clear mismatch between why purchasers walk away from deals and why providers think their potential customers abandon deals. Our surveyed cohort of cloud providers clearly outlined two reasons why cloud deals collapse during negotiations – pricing and, though harder to define, political, cultural and regulatory restrictions. In contrast, cloud purchasers rarely mentioned these factors.

The survey data suggests that cloud providers are potentially missing a trick. Rather than compromising on price (certainly where price isn't going to be the distinguishing factor to win the sale), vendors could minimise deal breakdowns by being more accommodating on contractual terms relating to data residency, security breach reporting and subcontracting as well as considering key areas of concern for customers such as SLAs and liability (see below).

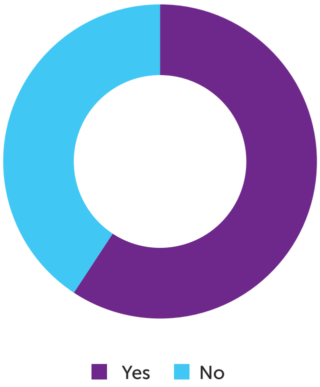
What are typically customers' most common reasons for walking or almost walking away from cloud deals? (Providers)



Contract negotiation best practice

Data protection terms are paramount
Cloud deals often break down during negotiations because agreement can't be reached on terms and conditions. Almost 60% of surveyed cloud purchasers who walked away from deals during negotiations did so because terms and conditions couldn't be agreed.

Has being unable to reach agreement on terms and conditions ever caused you to walk away from a cloud deal which was part way through negotiations? (Purchasers)



By far the most difficult point to reach consensus on is data protection terms - half of surveyed cloud purchasers that ducked out of a cloud deal due to term negotiation failure did so specifically because data protection terms could not be finalised. Acceptable SLA terms and liability terms were the joint second most common difficult areas to reach agreement on.

Which data protection terms are most important? Two terms that stand out to cloud purchasers are:

1. A requirement of cloud vendors to provide an obligation to securely delete data, including personal data, from cloud facilities within a specified time frame and to certify in writing when done; and
2. A requirement of cloud vendors to allow limited security testing/penetration testing.

Eight out of ten surveyed cloud purchasers require that these two security measures are agreed to before entering into a cloud deal. Encouragingly, most (77%) surveyed cloud providers are willing to provide this.

Penetration testing isn't typically required by law, albeit the FCA and other regulatory bodies have provided interesting guidance in this area. Instead, cloud purchasers seek to conduct penetration testing because they are required to conduct appropriate security due diligence when data is outsourced.

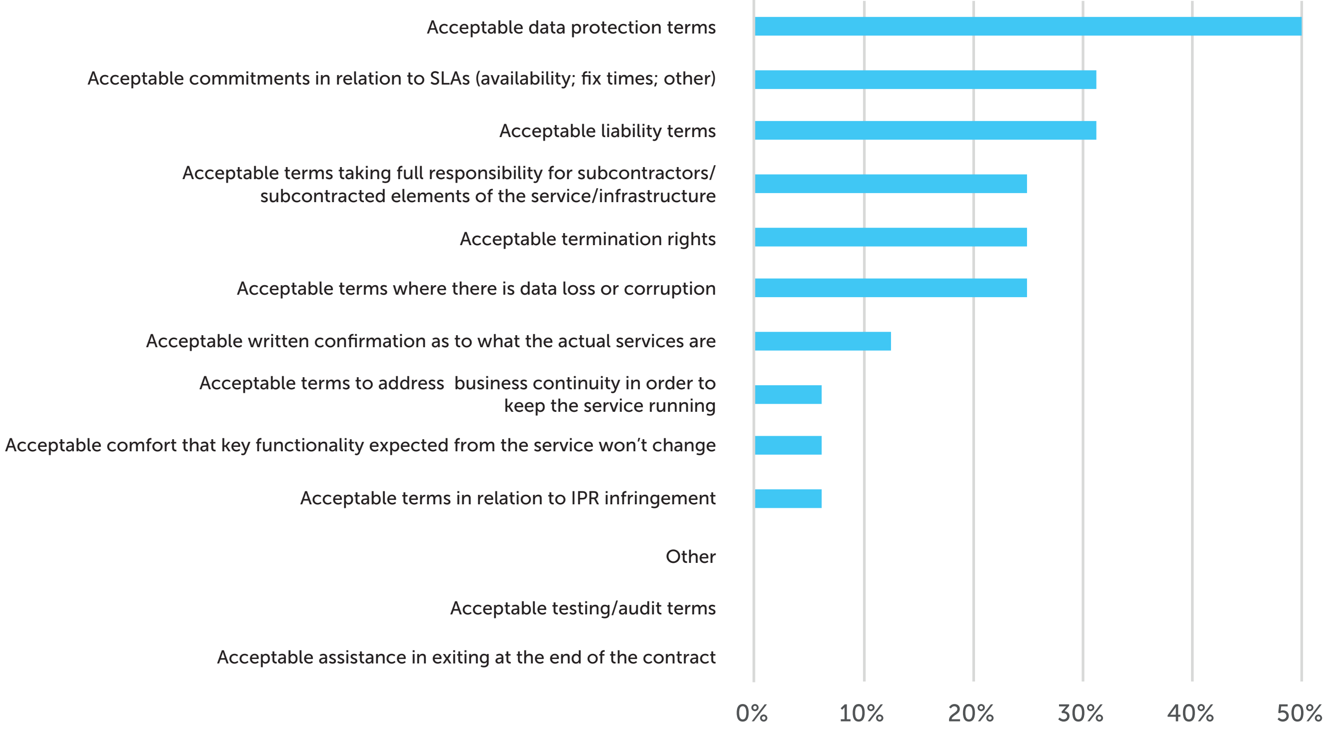
Fewer purchasers (65%) require cloud vendors to tailor security processes and controls to their requirements in key cases only and even fewer (56%) require cloud vendors to completely or mainly tailor their security processes and controls to meet internal security requirements.

Naturally, the level of security terms and conditions cloud purchasers require depends on the industry they operate in. Highly regulated sectors such as healthcare and financial services that deal with large quantities of sensitive personal data will likely require more comprehensive security provisions.

The extent to which providers will be willing to meet customers' security requirements depends on the type of cloud solution being negotiated. In Eversheds' experience of acting on both sides of the deals, some customers want suppliers to comply completely with their security policy. Clearly, that might work well with a private or even a hybrid cloud solution, but it's very hard to expect or achieve that with public cloud. That's not to say that a customer cannot achieve the level of security it wants by configuring the solution. However, asking for a warranty around compliance against the policies in the contract is understandably problematic for public cloud suppliers to provide.

Service level agreements and liability clauses must be thought through
As mentioned earlier, failure to agree adequate SLAs and liability clauses are common reasons why cloud deals break down during negotiations. But what level of SLA and

What were the reasons for walking away from the deal? (Purchasers)



liability clause is typical in a cloud contract? It obviously depends on the type of deal and the purchaser's individual requirements, but there is consensus among surveyed cloud purchasers that liability to cover likely losses and their likely value is expected from the supplier. This might include losses resulting from regulator fines, to the extent the law will allow recovery of these, and personal data compensation claims following a security breach.

However, the reality of the situation is that this level of loss protection is often not available – only 27% of surveyed cloud providers typically provide this to clients.

A sizeable minority (39%) of customers expect cloud providers to agree to upfront SLAs. They are likely to have much more luck in securing this – two thirds of surveyed cloud providers are typically willing to provide this.

A common area of difficulty regarding SLAs is that cloud providers often state in a contract that they will use "reasonable endeavours" or "commercial efforts" to meet their SLAs, that SLAs are only targets, or that they are the sole remedy for losses caused. This language is often used even when the sales literature suggests these SLAs are a key feature of the service to be expected. Put simply, the promise and the contract do not match.

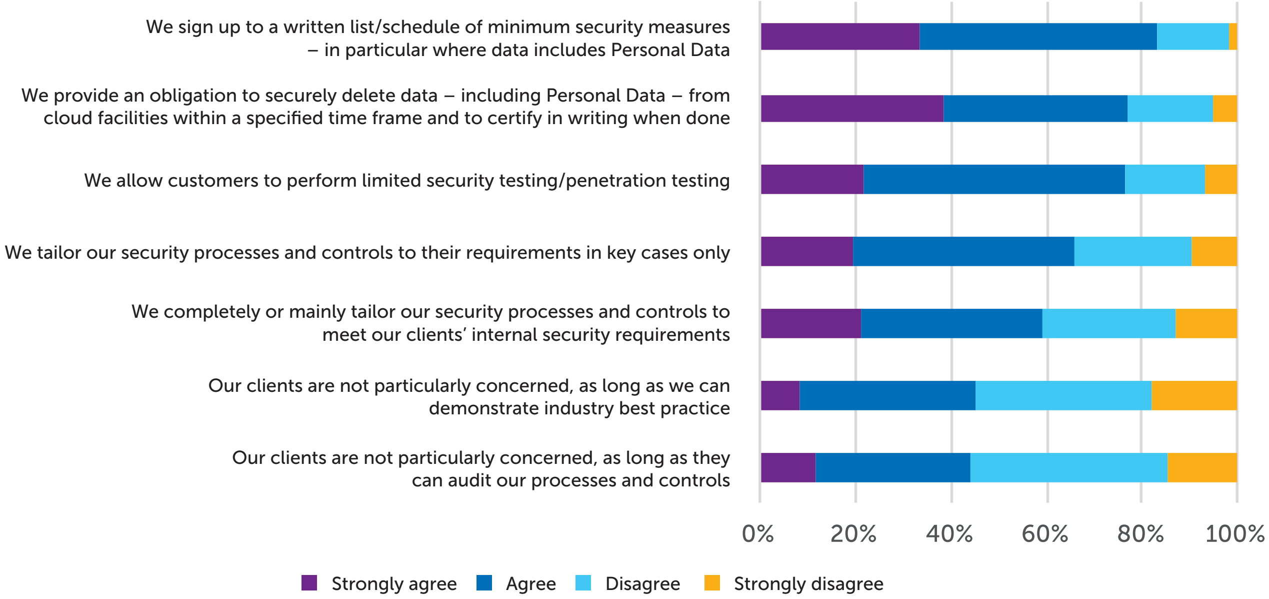
Customers have walked away from deals where suppliers are not willing to give assurances around the level of service and the time needed to fix issues such as availability and functionality. Customers particularly struggle with this when the spend is high and/or the solution highly tailored, such as a private or very tailored hybrid solution. In Eversheds' experience, this remains perhaps one of the most fiercely negotiated areas of the contract and can potentially waste a lot of deal time.

A significant discussion point is also what liability provisions are in place when there is an outage, data loss or corruption. Again, the appropriate level of contractual comfort depends on the type of cloud deal and the risk tolerances of the purchaser and supplier. It seems from the findings that customers' willingness to accept outages liability may depend on the price and type of cloud service. That said, our survey data reveals a fundamental mismatch between what customers expect to be written into their contract regarding outages and what providers are willing to agree to.

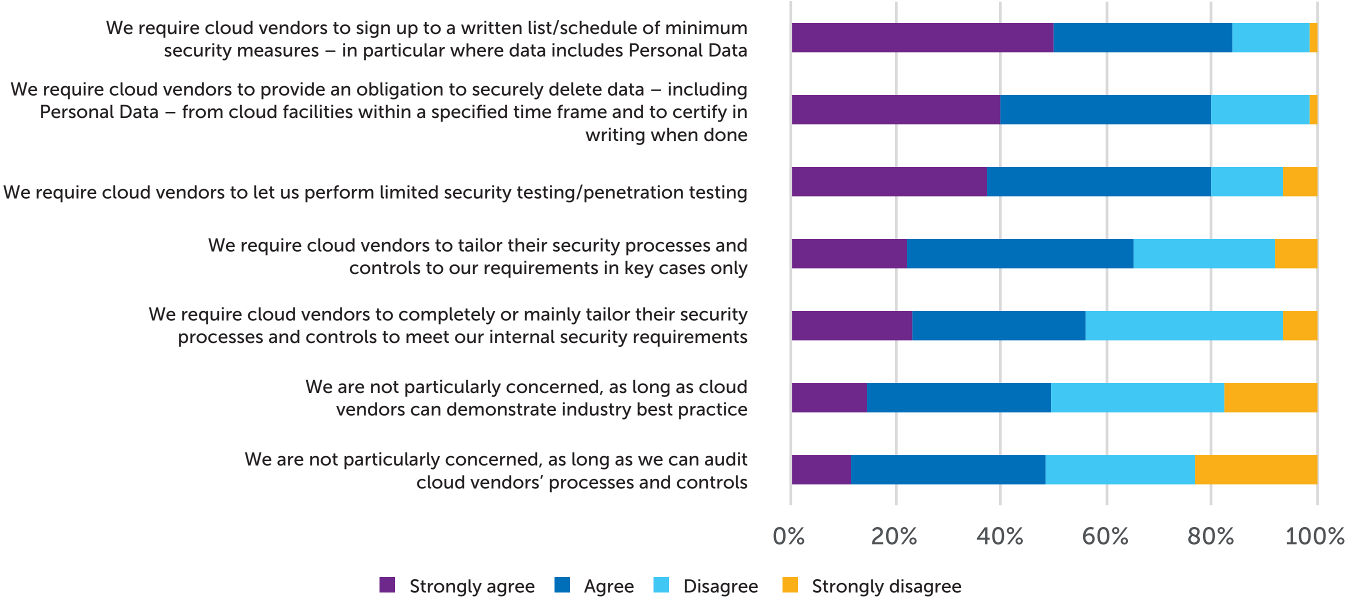
For example, 60% of surveyed cloud purchasers expect the right to terminate the contract quickly and without charge to be written into the contract if there are a number of outages in any month exceeding a set period. However only 39% of cloud providers provide this level of contractual comfort to clients. Instead the level of comfort most providers (55%) offer is a commitment to get the services back up and running within a set time. Some customers accept this more easily where there is little or no cost to exit the service in a "doom and gloom" situation. If this cost is significant, only having to get the service back up and running swiftly is a step too far for some of the customer-base.

Almost half (48%) of surveyed cloud customers also require service credits to be payable, which fully or significantly recompenses them for losses resulting from an outage.

To what extent do you agree with the following statements about the extent to which you tailor your security processes and controls for clients? (Providers)



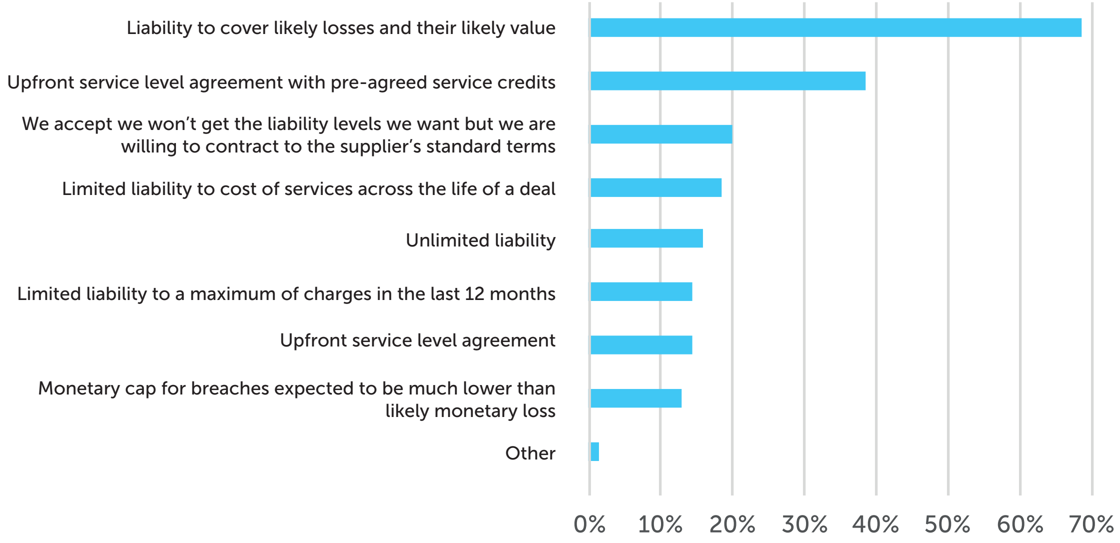
To what extent do you agree with the following statements about the extent to which you require cloud vendors to tailor their security processes and controls to your requirements? (Purchasers)



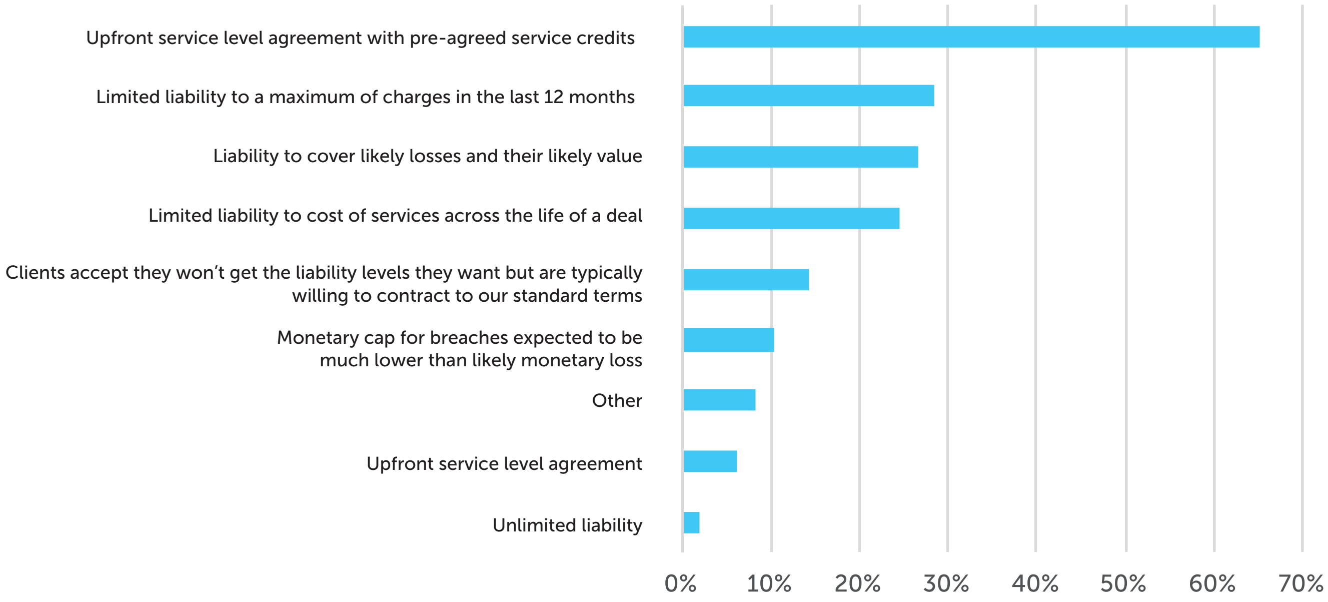
However, only 20% of cloud providers provide this level of contractual comfort. Given the service credits are often not high in value, vendors may be missing an easy differentiator here.

Of course, for ultra-critical business functions, customers not only need contractual comfort with what happens when things go wrong, but a practical solution to maintain the service. "If the outsourcing is something that is important and significant to its business it will focus more on having a backup solution and contingency plan in place to mitigate against any outage," notes Simon Gamlin.

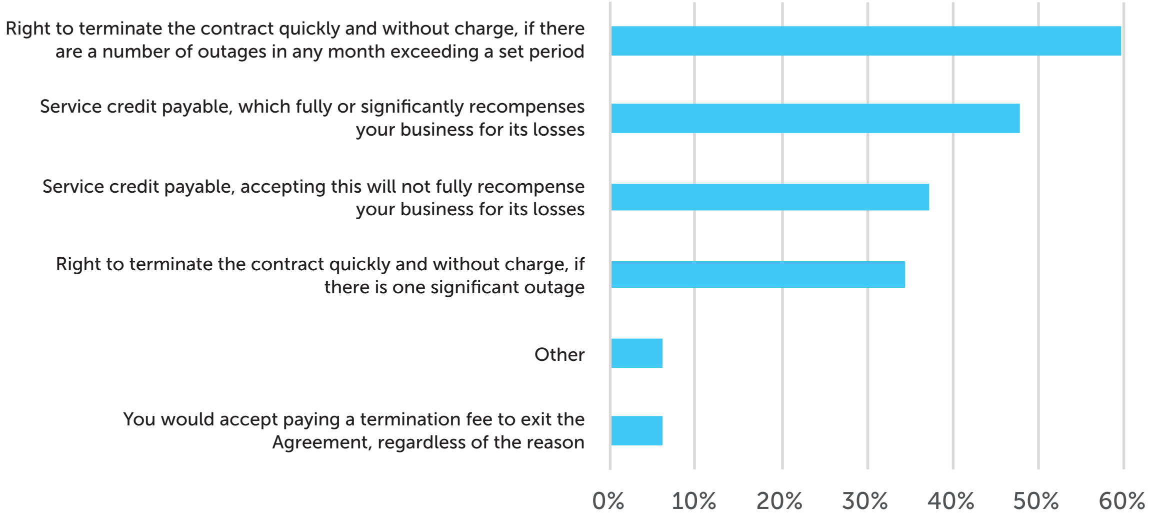
What level of contractual liability protection against loss best describes what you would expect from a cloud supplier before signing up? (Purchasers)



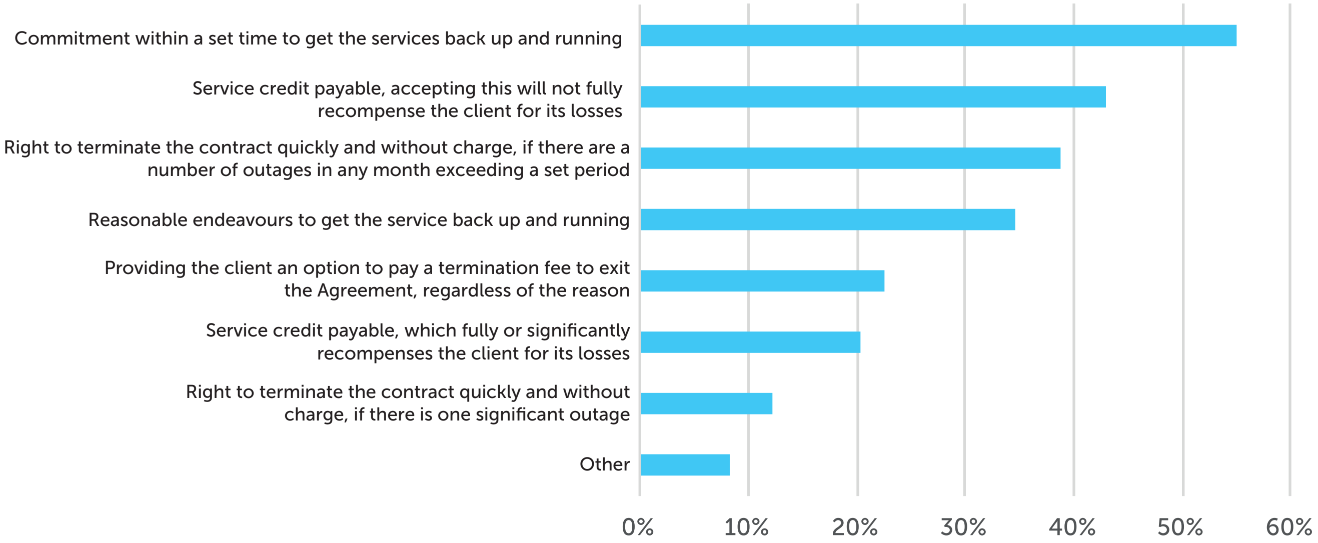
What level of contractual liability protection against loss best describes what you typically provide to clients? (Providers)



Your cloud service(s) experiences an outage (so that the cloud service could not be accessed or used for a period of time) – what contractual comfort would you expect to be written into your contract (without which you would not sign up)? (Purchasers)



What contractual comfort do you provide to your clients in the event of an outage (so that your clients cannot access or use your cloud service for a period of time)? (Providers)



Data liability – learning from Eversheds' experience

Liability for data loss and corruption is fiercely debated at the contracting stage and it is clear that this is an area that can lead to substantial tension in deals - 25% of customers have been unable to reach agreement on acceptable terms around data loss or corruption in a deal.

Interestingly, many customers do accept that cloud is not an "insurance policy" on the data side, but do wish for suppliers to be liable for data loss if it is a fair expectation as part of the service that the data will be protected to an adequate level and it is this "fair" level that is not met.

For example, in a recent negotiation, the supplier's legal team were arguing that the supplier should be able to *completely* exclude liability for data loss and data corruption even though the customer was paying for an enhanced hybrid service which included a paid for data back-up and a disaster recovery service. It transpired that the legal team was not aware that this service had been taken as an additional paid-for option. Needless to say, a pragmatic solution was eventually struck but the deal (which ran into a sum of US$ millions over five years) was nearly lost.

On the flip side, there are suppliers who clearly understand that data is king in the cloud and are clear and upfront about what their service will cover. These suppliers will often at least consider what a reasonable level of liability is for them to accept if data is lost or corrupted and it actually is their fault. Clearly, the level of risk a supplier should accept should reasonably be dependent on the type of solution and the commercial/ financial aspects of the deal. It is important that this is thought through on both sides early on.

One final observation relating to contracting is that customers want to understand how and when, from a technical viewpoint, data will be ported/transferred upon exit and the level of assistance that will be provided. Generally, the parties will reach amicable agreement on these areas but it is interesting to note that nearly 10% of customers have nearly walked away from deals when discussions reached what will happen at the end of the contract. This is an area where clear communication could save time on deals. Indeed, none of the surveyed recipients actually did walk away from a deal for this reason.

Industry trends – focus on M&A

M&A activity involving cloud companies has surged in recent years. According to M&A advisory firm Hampleton, some 40 cloud security firms were acquired in the first half of 2015, the most recent period for which this data is available. This is a significant increase considering that 45 acquisitions of cloud security firms were acquired during the entirety of 2013 and 2014. Of course, cloud security is only one specific sub-sector of cloud, but this trend illustrates a surge in M&A activity across the wider cloud computing market. Notable cloud M&A deals in 2015 include:

- Amazon Web Services' US$296 million acquisition of video delivery software provider Elemental Technologies in September 2015;

- Cisco Systems' acquisition (value undisclosed) of threat protection company OpenDNS in June 2015;

- Francisco Partners' US$438 million purchase of field service and workforce management solution provider ClickSoftware Technologies in April 2015.

Survey respondents are unanimous that M&A activity will continue apace – nine out of ten surveyed cloud advisors (law firms, financial advisors, consultants etc.) expect cloud services M&A to increase in the next 18 months. None predict a decrease.

Why is deal activity predicted to surge? The main reason, according to 46% survey respondents, is that M&A enables companies to fill gaps in their product set. This is more than double the number of respondents that identified any other factor as a driver for M&A.

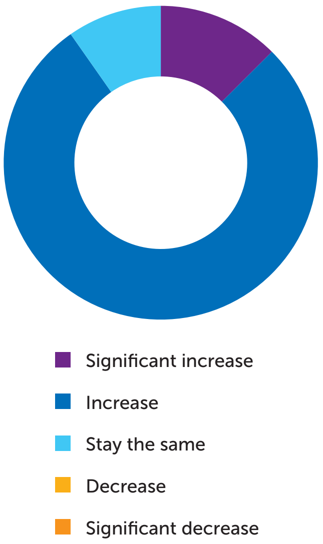
Of course, there are a number of challenges to executing M&A in this sector. Some 40% of surveyed service providers stated that identifying which cloud services will experience greatest demand is a 'primary' challenge to executing deals in this space. A further 23% identified 'integrating acquisitions into the group structure' as a significant challenge, and 22% stated that 'valuing cloud services companies, given customer contracts are typically short and easy to exit' is a challenge.

That said, there are also a number of factors unique to the cloud industry that make it easier for strategic investors to evaluate, execute and then integrate acquisitions. "There are a number of factors that have made cloud and Software-as-a-Service businesses attractive targets for both strategic acquirers and financial sponsors over the last few years," explained Alexis Scorer, Director at GP Bullhound. "SaaS businesses have much more predictable recurring revenue streams than older "perpetual license" businesses. Cloud software business also typically deliver significantly higher growth, driven by shorter sales cycles and market demand from the ongoing shift towards Enterprise SaaS adoption. SaaS release cycles are also dramatically shorter than for on premise software, allowing cloud businesses to be much more agile in responding to market needs."

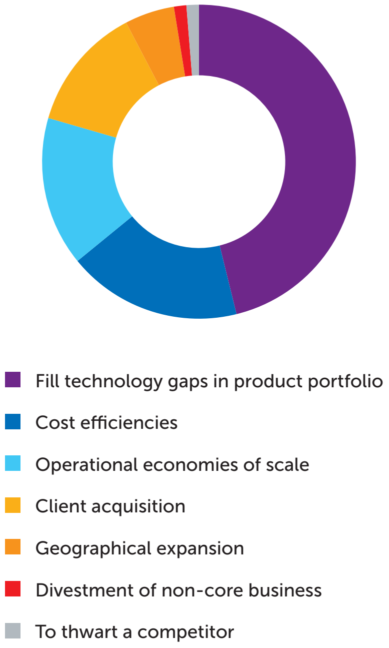
Various legal issues need to be considered deeply when acquiring cloud businesses, depending on the business rationale for acquiring the company. In addition to the usual set of M&A legal considerations, purchasers of cloud businesses need to consider that jurisdictional data protection regulations mean that cloud solutions developed in one country cannot simply be rolled out globally and that the technology behind the service offering will need considering in this respect.

Additionally, given the very nature of cloud contracts being scalable, it is harder to evaluate the potential customer revenue streams even if they are recurring. It is important for vendors to focus on termination rights, termination charges and minimum commitments in this respect.

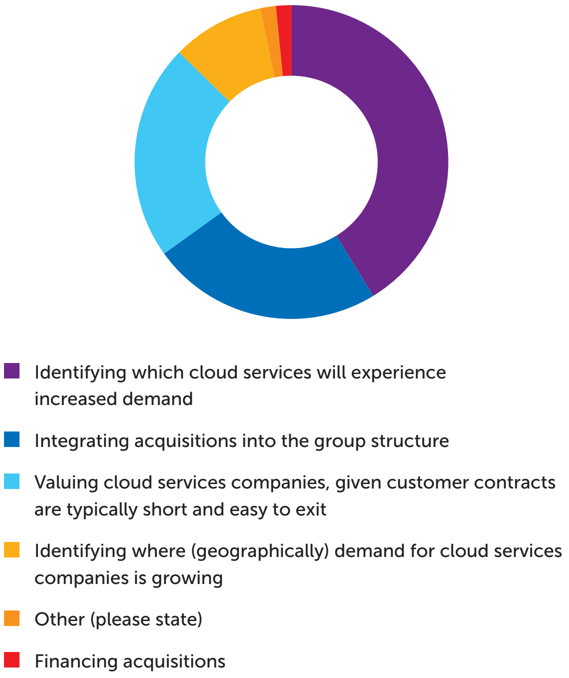
How do you expect the level of M&A in the cloud services sector to change in the next 18 months? (Advisors)



What will be the primary motivations for M&A activity involving cloud services companies during the next 18 months? (Advisors)



What are the primary challenges when acquiring cloud services companies? (Advisors)



About the research

The survey and report were written in collaboration with The Lawyer Research Service, a division of The Lawyer. The survey was undertaken in December 2015 and January 2016 and was completed by 350 cloud providers, purchasers and industry advisors worldwide.

To supplement the survey, interviews were conducted with the following individuals:

Industry executives:
Alexis Scorer, Director, GP Bullhound
Helen Kelisky, VP Cloud (UK & Ireland), IBM
Ashraf Abdelwahab, Director of Corporate Affairs, Gulf & Egypt, Microsoft
Mark Bennett, Executive Director, Head of IT Legal, Legal and Compliance, Nomura International
Alastair McAulay, Director of Disruptive IT, PA Consulting Group

Eversheds Partners:
Charlotte Walker-Osborn, Partner, Global Head of Technology, Media and Telecoms, Eversheds LLP (author with Thomas Sturge, Head of Research, The Lawyer)
Paula Barrett, Partner and Global Head of Privacy and Information Law, Eversheds LLP
Nigel Stamp, Partner, Head of Technology, Media and Telecoms, Asia, Eversheds LLP
Simon Gamlin, Partner, International IT Group and International Outsourcing Group Lead, Eversheds LLP

Contacts

Charlotte Walker-Osborn
Global Head of Technology,
Media and Telecoms

T: +44 121 232 1220
M: +44 779 907 5756
charlottewalker-osborn@eversheds.com

Paula Barrett
Global Head of Privacy and Information Law

T: +44 20 7919 4634
M:+44 777 575 7958
paulabarrett@eversheds.com

Simon Gamlin
International IT Group and International
Outsourcing Group Lead

M: +44 776 289 6040
T: +44 20 7919 4689
simongamlin@eversheds.com

Nasser ali Khasawneh
Head of Technology, Media and
Telecoms, Middle East

T: +97 14 3 89 70 03
M: +971506553198
nasseralikhasawneh@eversheds.com

Nigel Stamp
Head of Technology, Media
and Telecoms, Asia

T: +852 2186 3202
M: +852 9187 3911
nigelstamp@eversheds.com