VERITAS™

Data Management in a Multi-Cloud World:

Professional Services Edition

Executive Summary

Historically, the primary purpose of cloud technology in a business context would have been as a means of extending data storage capabilities, but in a modern-day context it brings with it almost endless potential in terms of supporting effective business operations.

However, despite the many benefits the cloud can deliver, the rising utilisation is not without its challenges, especially in the context of a post-pandemic world and when thinking of highly regulated industries such as professional services.

These challenges relate not only to the more traditional cloud concerns such as security, but also to vital areas within data management and data protection. For many organisations, data backup capabilities need considerable improvements, there are concerning gaps in data visibility, and there is also ample room for improvement within scalability of data management and protection.

Solutions exist which can help organisations to achieve better results in all of these areas, and it's therefore important that such solutions are explored. Failure to improve in these areas could leave organisations vulnerable to consequences including regulatory breaches, business disruption or financial penalties.

This report focuses on a recent quantitative research study conducted with UK and Ireland IT decision makers (ITDMs). It explores how professional services organisations are approaching cloud adoption, where the key challenges and apprehensions exist, and how organisations can look to overcome these challenges through making improvements to their approaches to data management and data protection.

Data Management in a Multi-Cloud World
Key findings

Click on a key finding to read more

48%

of data in surveyed ITDMs' organisations is stored or managed in the public cloud at present, expected to rise to 75% in five years' time, on average

64%

of respondents say that, thinking since COVID-19, moving more apps/data to the cloud is a top three priority for their organisation – higher than any other priority

92%

identify at least one application or data source that their organisation is unlikely to move to public cloud – security concerns (72%) are the most likely reason for this

68% agree that legislation and regulation makes data management more challenging

On average, respondents estimate that 29 working hours per week are spent in their organisation finding and retrieving data specific to regulatory requirements (e.g. SARs)

In the context of data backups, only a minority of surveyed ITDMs state that their organisation already has infrastructure that enables: storing backups across different locations (31%), having a consolidated on-premises and cloud solution (21%), being able to backup all workloads equally effectively (13%), and automatic discovery of workloads and creation of backups (9%)

37%

of respondents' organisations have full visibility with regards to regulatory requirements in relation to unstructured data

82%

highlight that scaling cloud backups and disaster recovery as cloud deployment grows could be easier, while 60% agree that an inability to scale cloud deployments effectively will hold organisations back

88%

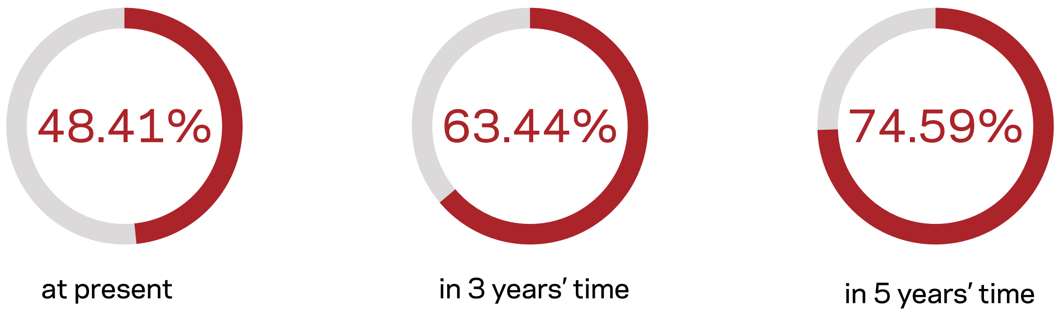
utilise multiple different vendors or solutions in unison within their data protection infrastructure

<< Key findings

Cloud adoption is on the rise in professional services organisations

It should come as no surprise to see that cloud adoption in modern organisations within the professional services space is on an upward trajectory. Surveyed UK and Ireland IT decision makers from professional services organisations estimate that approaching half (48%) of the data in their organisation is stored or managed in the public cloud at present, on average, and this figure is expected to see a notable rise to 75% in the next five years.

Average percentage of data stored/managed in the public cloud

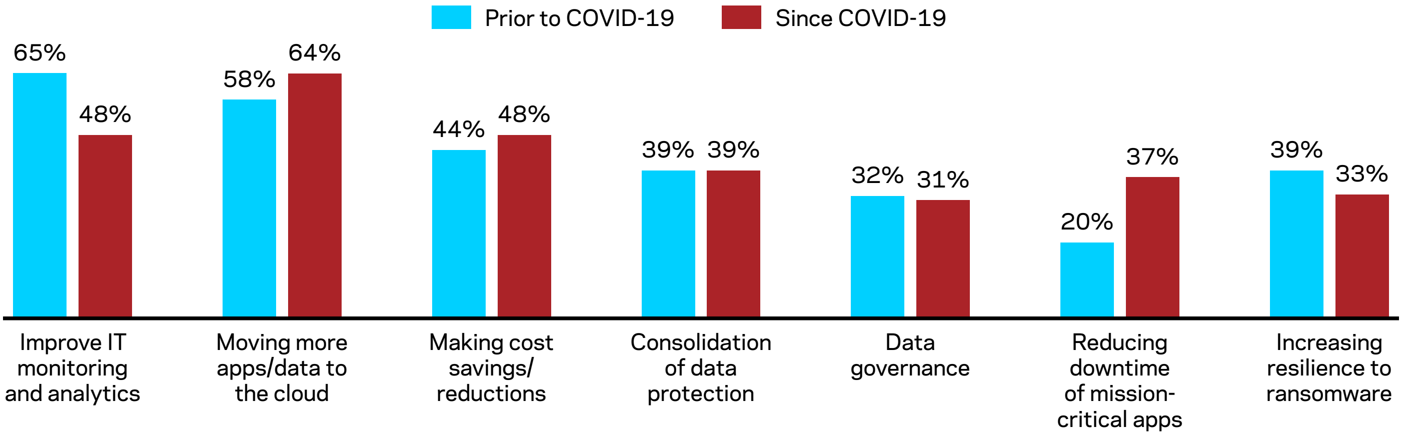


What percentage of your organisation's data would you estimate is stored/managed in the public cloud at present and will be in the following timeframes? [100]

Considering the vast quantities of data that modern-day organisations will be managing, this represents a huge cloud undertaking and immediately highlights the importance of discussing cloud in any conversation about data management and data protection.

The COVID-19 pandemic has accelerated organisations' progress towards a more cloud-centric IT environment in many cases, while also resulting in a series of other adjustments in business priorities. When thinking prior to the pandemic, 58% of respondents identified moving more apps and data to the cloud as being one of their organisation's top three business priorities. Yet thinking since COVID-19 commenced, approaching two thirds (64%) place it in the top three – higher than any other priority.

Organisations' top three priorities prior to and since COVID-19



Showing the proportion of respondents that place the above in the top three priorities for their organisation when thinking prior to COVID-19 and since COVID-19 [100]

Meanwhile, while cloud utilisation rises, examples such as improving IT monitoring and analytics are less likely to be in respondents' top three priorities since COVID-19 (48% compared to 65% prior to COVID-19), something which is potentially cause for concern. It begs the question – as organisations do become more cloud-centric, are they assuming that this reduces their need for effective IT monitoring and analytics as they move away from physical infrastructure? In reality, this would not be the case. Instead, organisations would need to adjust their IT monitoring and analytics capabilities to ensure that they work as effectively as possible across all systems and across all deployments.

A similar downward trend is true for increasing resilience to ransomware (33% compared to 39% prior to COVID-19), another area that has slipped slightly down the priority list during the pandemic. Again, this is a worrying finding, with ransomware attacks being relatively commonplace in UK organisations[1]. In addition, as a result of the widespread shifts in how organisations have operated throughout 2020, the threat level for cyber attacks such as ransomware is arguably higher than ever before, something that organisations must keep in mind.

Most organisations are needing to move full steam ahead with further implementation and utilisation of cloud-based deployments in order to remain agile and operational enough during the pandemic and its aftermath. But at the same time, they must make sure that their data management and data protection is able to keep pace, whether thinking about IT monitoring and analytics, ransomware resilience, or otherwise. Failure to successfully negotiate this balancing act can come with sizeable consequences.

[1] Veritas Ransomware Resiliency Research for EMEA

<< Key findings

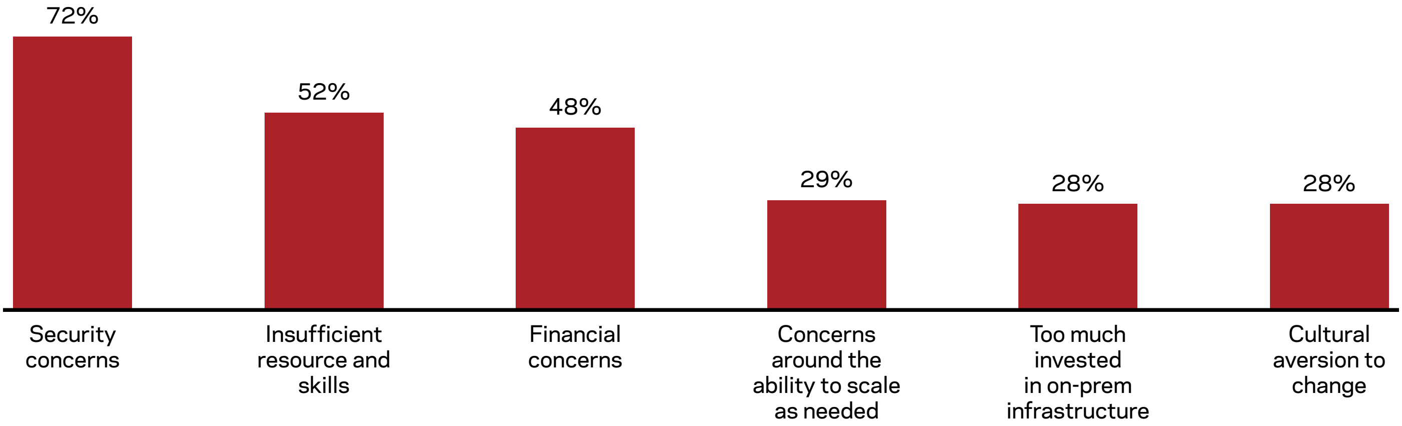
Apprehensions around cloud-based deployments

While the gradual shift towards increased cloud utilisation continues in professional services organisations, this is not without certain apprehensions. Many acknowledge that the move to cloud is not always straightforward and doesn't necessarily provide a remedy to every possible IT challenge. In fact, 92% of surveyed ITDMs identify at least one application or data source that their organisation would be unlikely to move to public cloud.

The most likely factor contributing to this is security concerns (72%). As data becomes an increasingly sizeable and valuable asset for organisations over time, they will inevitably have concerns around anything that might place this data under a greater degree of risk.

92%
of ITDMs identify at least one application or data source that their organisation would be unlikely to move to public cloud

Factors preventing moving certain apps and data to public cloud



What factors prevent your organisation from moving certain applications and data sources to public cloud? [92] Asked to respondents whose organisation would be unlikely to move certain applications or data sources to public cloud

During a time when organisations are so acutely aware that a data breach or cyber security blip could spell disaster for their organisation, it's understandable that security concerns remain front of mind. In fact, three in ten (30%) respondents admit that their organisation has been a target of at least one cyber attack (e.g. a ransomware attack) in the last 12 months, a figure that is likely to be even higher in reality. Yet, close to three quarters (73%) admit that their organisation needs to improve their approaches to dealing with such incidents.

30%

admit that their organisation has been a target of at least one cyber attack (e.g. a ransomware attack) in the last 12 months

In addition, this research found that all (100%) respondents' organisations attach at least some level of importance to understanding data risk – the risk that organisations may face consequences as a result of poor data governance or management. In fact, 59% attach a high level of importance to this. However, this is not stopping organisations from hurrying towards cloud deployments despite identifying the potential security risks that come with them.

The benefits of cloud use are clearly deemed surplus to the potential drawbacks. However, while the consequences of ineffective data management and regulatory non-compliance are clear to see and the potential for cyber attacks remains high, it's evident that organisations' data management and data protection choices are arguably more important than ever.

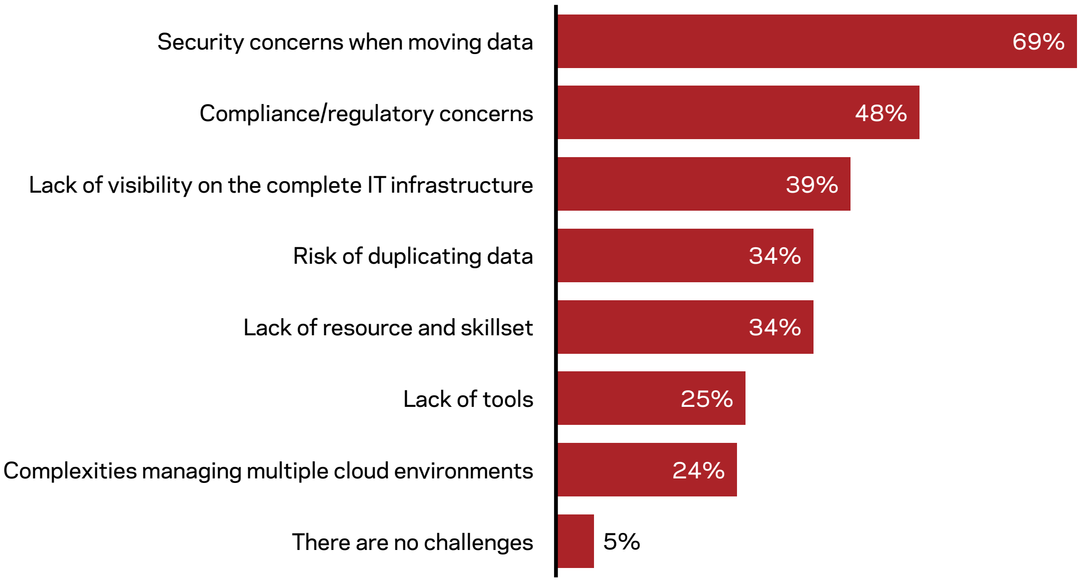
The impact of regulations on professional services organisations

When thinking about moving certain applications and data into and out of cloud environments, as many professional services organisations inevitably will be, a series of additional challenges are presented.

Again, it's the security concerns when moving data (69%) that is most frequently identified as a challenge by respondents. But, in addition, around half (48%) identify compliance and regulatory concerns here too, something that makes a lot of sense in the context of a highly regulated industry, such as professional services. In fact, over two thirds (68%) of respondents agree that legislation and regulation makes data management more challenging for their organisation.

68%
agree that legislation and regulation makes data management more challenging for their organisation

Challenges encountered when moving applications or data into and out of cloud environments



When thinking about moving applications and data into and out of cloud environments in your organisation, what kind of challenges does your organisation encounter? [100] Asked to respondents whose organisation is storing/managing at least some data in the public cloud at present

Looking at a more specific example within regulatory compliance, consider subject access requests (SARs) since the introduction of GDPR in 2018. An overwhelming majority (99%) of respondents' organisations have a formalised process for managing SARs, but for 82% this process is at least partially manual. It's therefore no real surprise to see almost all (98%) respondents admitting that their organisation could improve its approach to managing and processing these.

98%

of respondents admit that their organisation could improve its approach to managing and processing subject access requests (SARs)

For large organisations, the time and resource spent ensuring adherence to regulations can quickly add up. Respondents estimate that, on average, their organisation spends 29 working hours every week finding and retrieving data specific to regulatory requirements (e.g. SARs) – close to the equivalent of a full-time employee's working hours each week. On top of that, a further 26 working hours are estimated to be spent analysing that data. These are simple estimates but could in reality amount to much higher figures, and this is time and resource that could be being spent so much more effectively elsewhere in the organisation.

Organisations do not have a choice on regulatory compliance and failing to adhere to standards can result in crippling punitive fines. It is therefore essential that organisations adopt tools and processes that enable their data management to be as effective as possible, even in cloud environments.

<< Key findings

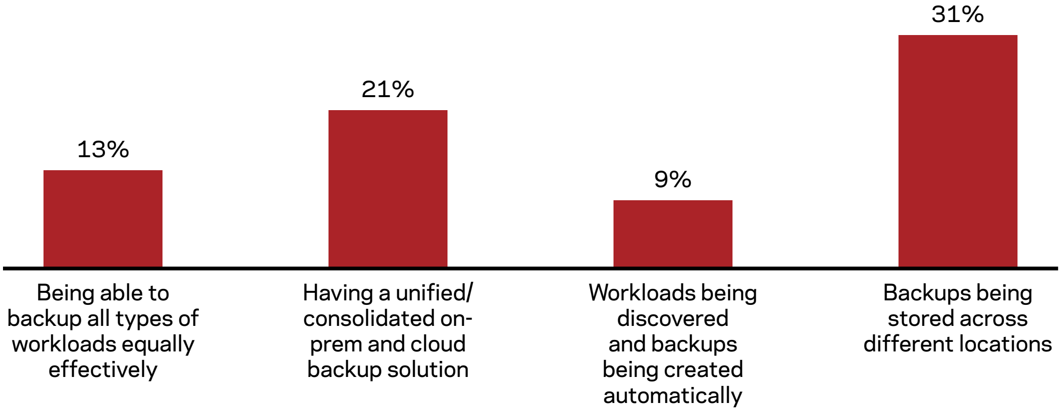
Areas for improvement within data management and data protection

Before organisations are able to make progress in terms of their overall data management and data protection, they must identify which key areas have room for improvement.

Data backups

One area that many organisations must review is how they approach data backups. The majority of surveyed ITDMs highlight it as being either absolutely essential or very important that their organisation is able to: backup all workload types equally effectively (91%), work with a unified on-premises and cloud backup solution (86%), discover workloads and create backups automatically (79%), and store backups across different locations (77%). However, despite the clear value associated with these backup elements, only a minority of respondents feel that their organisation already has infrastructure that fully enables them and does not leave any room for improvement. As an example, only 13% of respondents stated this to be true for being able to backup all workload types equally effectively in their organisation.

"No improvements needed - our current infrastructure already enables this"



Showing the proportion of respondents that believe their organisation does not need to improve and can already achieve the above with their existing data backup infrastructure [100]

Areas considered essential or very important for data backups:

91%
Being able to backup all types of workloads equally effectively

86%
Having a unified/ consolidated on-prem and cloud backup solution

79%
Workloads being discovered and backups being created automatically

77%
Backups being stored across different locations

Beyond this, there's a need for organisations to re-evaluate how cloud-based critical workloads are backed up in their organisation. The majority (85%) of respondents report that their organisation leaves this backup responsibility with their cloud service provider (CSP), an approach which is fine if the CSP actually is backing up these important workloads. Yet often this is an assumption that gets made without confirmation. In many cases, CSPs may not be backing up all workloads that run on their platform – this is something that organisations ought to be wary of and reviewing in order to avoid any valuable workloads being left vulnerable.

Organisations must make certain that their backup capabilities are comprehensive, automated, and functional regardless of deployment method. As part of this, they should review whether their CSP's T&Cs cover backups for all cloud-based data or not. This will help them to ensure a fast and effective recovery if a disruptive incident occurs.

Visibility

Data visibility is another vital element within organisations' data management, especially when considering the highly regulated nature of professional services organisations. However, it is only 37% of respondents that believe that their organisation has full visibility over unstructured data when considering their existing tools and processes.

For the rest, visibility is deficient at least to some extent, and this is not good enough. Whether it is a case of considerable visibility gaps or very small ones, organisations run a very real risk of finding themselves non-compliant with regulations.

Only 37%

believe that their organisation has full visibility with regards to compliance and regulatory requirements of their unstructured data

Meanwhile, 67% admit that their organisation still utilises in-house spreadsheets as part of their data management strategy. This remains very common, but it is certainly not an effective way of managing data accurately and in real-time. Data is such a valuable resource for modern organisations but approaches such as this severely hinder the utilisation and analysis potential that it can provide.

Organisations should explore data management solutions that already exist which facilitate the all-compassing data visibility that is needed in order to maximise data use and stay compliant with regulations.

Scalability

Another important area within data management and data protection is scalability, particularly when considered against the backdrop of growing cloud deployments within most modern organisations. While almost all (94%) respondents' organisations are able to scale cloud backups and disaster recovery as cloud deployments grow, over four fifths (82%) of respondents admit that this could be easier. This is something that could and should be simple enough, but clearly is not in many cases.

Meanwhile, over six in ten (63%) acknowledge that scaling data protection and data management is set to be a big challenge over the next five years. With the volume of data growing in general in organisations and this data being spread increasingly across different deployments, this is understandable. In addition, 60% believe that an inability to scale cloud deployments effectively will hold organisations back, something that no organisation can afford to endure, particularly in a post-pandemic landscape where any competitive disadvantage could be treacherous for a business.

63%
believe that scaling their data protection/management solutions is a big challenge for the next five years

60%
agree that an inability to scale cloud deployments effectively will hold organisations back

Most organisations would clearly benefit from a data protection and management solution which is not inhibited when it is time to scale operations up or down, so that they can embrace growing volumes of data and growing cloud utilisation rather than see this as a challenge.

Using multiple vendors

Something that is likely to be a key contributor to many of the struggles mentioned so far in this section is organisations' use of multiple different vendors in unison, something that approaching nine in ten (88%) respondents' organisations do as part of their data protection infrastructure. In reality, this approach can bring with it a whole host of additional challenges.

First, there will most likely be an increase in the overall complexity of the data protection environment when working across different vendors or solutions. This includes the complexity that comes with deploying and maintaining different tools as well as that which comes with keeping all relevant staff members trained and up to speed on how best to use each tool.

In addition, there's also the potential for this approach to bring with it heightened risk. Data protection gaps are more likely in organisations where a multitude of different tools and vendors are used. With this being the case, there is a greater possibility that overcoming things such as data loss or a spell of downtime is more challenging and time-consuming for organisations, something that they really cannot afford.

Organisations ought to aim for unification of their data protection and data management vendors where possible. This can result in simplified and yet overall, more effective and lower risk performance across solutions.

Conclusion

Cloud adoption is expected to continue rising in the coming years, something that the COVID-19 pandemic has only fast-tracked, and this will no doubt be inviting additional complexity and challenge into organisations' data protection and data management.

This is in addition to a series of stubborn, pre-existing apprehensions that exist amongst surveyed IT decision makers in relation to cloud deployments in general. These are primarily linked to security concerns but are further heightened by the wide-ranging series of rules and regulations that govern the operations of professional services organisations.

At the same time, there are several important areas where considerable room for improvement exists in terms of data protection and data management in many organisations. Backup processes are often not automated, cloud-centric or complete enough, data visibility is not good enough, and scalability of data management as cloud deployments grow leaves a lot to be desired.

On top of this, many organisations are still working across multiple distinct vendors and solutions as part of their data protection and data management infrastructure. While this is generally the result of good intentions, it is often something that ends up being a key contributor to and a key amplifier of data protection and management challenges.

In an ideal world, organisations should aim to have a single vendor that provides their entire suite of tools, from backups and disaster recovery to IT monitoring and analytics. This unification of tools would mean that they work together more effectively, thereby simplifying the overall process of looking after data. In turn, this would likely improve IT robustness, resilience and reliability. The overall impact of this would be organisations that are better placed to embrace cloud deployments in the future without apprehension, rather than viewing them as a cause for concern.

VERITAS™

ENTERPRISE DATA SERVICES

PLATFORM

AVAILABILITY

PROTECTION

INSIGHTS

ABOUT VERITAS

Veritas Technologies is a global leader in data protection and availability. Over 50,000 enterprises—including 99 of the Fortune 100—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas supports more than 500 data sources and over 150 storage targets, including 60 clouds. Learn more at http://www.veritas.com

ABOUT VANSON BOURNE

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com

METHODOLOGY

Veritas commissioned independent technology market research specialist Vanson Bourne to undertake the quantitative research upon which this report is based. A total of 100 UK and Ireland IT decision makers were interviewed in November 2020. Respondents were from **professional services** organisations with at least 500 employees. Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.