The rise of multi-cloud: Combatting misconceptions and realigning data management responsibilities
CLOUD-FIRST MENTALITY

Today, many organisations are taking a cloud-first approach when it comes to deploying new applications and workloads. The majority (56%) of senior IT and business decision makers report that their organisation operates with a cloud-first mentality and three quarters (75%) state that their organisation currently works with infrastructure as a service (IaaS) cloud service providers.

Approach to applications and workload deployment

RISE OF THE MULTI-CLOUD

Multi-cloud is increasingly becoming a key component of most organisations’ IT strategy. Two thirds (67%) of respondents’ organisations use or plan to use two or more cloud service providers for IaaS, while a quarter (25%) plan to use four or more. On average, those organisations already working with IaaS providers have done so for four years, with more and more organisations expected to follow a similar path to a multi-cloud world in the future. However, with this approach, organisations must pay close attention to selecting service providers that are right for their business and their specific IT requirements.

Adoption of Cloud Service Providers for IaaS

Key considerations and use cases

Organisations understand the value a cloud provider offers in reducing the organisation-driven IT footprint and increasing business agility. They are eager to reduce recurring costs such as those associated with storing massive volumes of secondary data on a long term basis across multiple clouds. But when it comes to choosing cloud partners, organisations aren’t just focused on cost as a business driver. In fact, only 40% of respondents rank pricing as one of their top three selection criteria. More than half of respondents (60%), state that they are most concerned about data privacy/security and compliance when it comes to selecting a cloud service provider. This is not surprising given that, with the EU’s General Data Protection Regulation (GDPR) on the horizon, it is critical that data is protected and not exposed to potential breaches. Organisations are also very concerned about how their workloads will function in the cloud – both in terms of performance (49%) and resiliency/uptime (43%). For organisations to both comply and compete successfully in today’s crowded marketplace, they need to ensure that business disruption is kept to a bare minimum.

Analysis of the number of cloud service providers that respondents’ organisations currently or plan to work with for IaaS consumption.
Key factors in selecting a cloud service provider

Which of the below areas are of most importance to your organisation when it comes to selecting a cloud service provider? Combination of responses ranked first, second and third.

<table>
<thead>
<tr>
<th>Area</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data privacy/security and compliance</td>
<td>60%</td>
</tr>
<tr>
<td>Workload performance</td>
<td>49%</td>
</tr>
<tr>
<td>Workload resiliency/uptime</td>
<td>43%</td>
</tr>
<tr>
<td>Data protection/backup</td>
<td>42%</td>
</tr>
<tr>
<td>Pricing</td>
<td>40%</td>
</tr>
<tr>
<td>Data visibility</td>
<td>27%</td>
</tr>
<tr>
<td>Data and workload portability</td>
<td>17%</td>
</tr>
<tr>
<td>Optimised storage</td>
<td>13%</td>
</tr>
</tbody>
</table>

Responsibility for data protection

As organisations move to the cloud, many may incorrectly believe their cloud service provider holds the principal responsibility for data protection – over eight in ten (83%) believe that their organisation’s cloud service provider takes care of protecting their data in the cloud. This is often not the case. In addition, over half of respondents see responsibility for the secure transfer of data between on-premises and cloud (54%) and backups of workloads running in the cloud (51%) as sitting primarily with their cloud service provider. So, are organisations again leaving themselves exposed to additional risks?

Responsibility for application uptime

Around six in ten believe that the cloud service providers are responsible for ensuring the uptime of workloads running in the cloud as well as for the performance of workloads running in the cloud (58%). Furthermore, most respondents (83%) believe that their organisation’s cloud service provider takes care of ensuring workloads and data are protected against outages. With massive repercussions to any business if they incur a service outage, such as loss of profits, revenue and customers, it’s imperative that organisations understand that they probably own primary responsibility for business uptime even for applications running in the cloud.

MISCONCEPTIONS OF DATA MANAGEMENT

With organisations embracing cloud technologies and increasingly selecting multiple cloud service providers to advance their cloud journey, it is critical that enterprises understand who ultimately owns responsibilities for data management in the cloud. Our research shows that many organisations believe they can fully offload data management responsibilities to the cloud service provider, leaving themselves exposed across multiple areas. However, the Veritas legal team reviewed contracts from multiple public cloud service providers to help Veritas understand what customers and cloud service providers are responsible for with respect to data management in the public cloud. Despite customers’ belief that cloud providers hold the responsibility of data management, findings from the Veritas legal team show that cloud service provider contracts usually place data management responsibility on customers. This research explores three areas of data management specifically: data privacy and compliance, data protection, and application uptime.

Responsibility for data privacy and compliance

Data privacy and compliance (60%) is the main area of importance for respondents’ organisations when selecting a cloud service provider. The vast majority (76%) of respondents believe that their cloud service providers take care of all data privacy and compliance regulations, which may be inaccurate, and around four in ten (38%) believe cloud service providers are responsible for auditing to ensure compliance. However, despite this apparent transfer of trust when it comes to compliance, only around six in ten (61%) respondents say that their organisation has written guarantees from their cloud service provider that data, including backups, will be permanently deleted upon contract termination. It’s critical that businesses ensure they are in compliance, regardless of where their data is stored, whether on-premises, in the cloud or in complex hybrid environments. With stringent compliance regulations pending around the world, including the European Union’s forthcoming General Data Protection Regulation (GDPR), businesses found to be in non-compliance could face significant penalties, extensive brand reputational damage, or both.

Responsibility for application uptime

Around six in ten believe that the cloud service providers are responsible for ensuring the uptime of workloads running in the cloud as well as for the performance of workloads running in the cloud (58%). Furthermore, most respondents (83%) believe that their organisation’s cloud service provider takes care of ensuring workloads and data are protected against outages. With massive repercussions to any business if they incur a service outage, such as loss of profits, revenue and customers, it’s imperative that organisations understand that they probably own primary responsibility for business uptime even for applications running in the cloud.

CHALLENGES WITH ADOPTION

Despite being driven to the cloud in anticipation of security, resiliency and operating cost advantages, challenges with adoption remain for most respondents and their organisations.

According to respondents, most (92%) organisations’ business strategies involve moving more infrastructure and workloads to the cloud over the next 12-24 months. Nearly a quarter of businesses (27%) plan to move all infrastructure and workloads to the cloud during that time period. However, organisations state they are facing serious challenges as they make this transition to the cloud, including: complexity of the migration (37%), limitations (36%), a lack of in-house skills (38%) and a lack of a clear strategy (32%) in their cloud migration. Many organisations turn to third parties for support and expertise. Over half (54%) use or plan to use consulting firms and around a third (36%) use or plan to use other vendor solutions.
Cloud outages
Most (94%) respondents are confident in cloud service providers’ abilities to protect workloads against outages, yet despite this, many respondents still report their organisation experiencing service disruptions. Over a third (36%) admit to having cloud service disruptions. As a result, service downtime (73%) is the most commonly reported consequence, and many also experienced a hit to customer satisfaction (46%) and loss of revenue (37%). On average organisations report experiencing approximately 22 minutes of downtime each month. Almost a third of all organisations (31%) have even faced more than 30 minutes of downtime per month.

Cloud lock-in
The majority (84%) of respondents report that cloud lock-in (the inability to easily transition to an alternative cloud or non-cloud hosted model) is a concern for their organisation. For almost four in ten (37%), this concern has inhibited accelerating cloud adoption. And despite the wide use (or planned use) of cloud service providers, it is interesting to note that only 8% of respondents report that they are happy with their current provider and would not choose to move. Only 12% of respondents say that their organisation can leave their cloud service provider immediately – for most (70%) it would take up to 12 months to detach themselves. Around a third (31%) do not have an established plan for data retrieval (or don’t know if their organisation does), if they opt to move back to on-premises or to another cloud.

Impact of cloud service disruption
What impact did your organisation experience as a result of cloud service disruption? Showing the results of the 432 respondents whose organisation has been impacted by a cloud service disruption.

Cloud migrations challenges
What challenges did your organisation face in its cloud migration? Below shows the results of the 593 IT decision maker respondents whose organisation is migrating systems to the cloud.

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of in-house skills</td>
<td>38%</td>
</tr>
<tr>
<td>Complexity</td>
<td>37%</td>
</tr>
<tr>
<td>Legacy technology limitations</td>
<td>36%</td>
</tr>
<tr>
<td>Lack of clear strategy</td>
<td>32%</td>
</tr>
<tr>
<td>Data siloes</td>
<td>27%</td>
</tr>
</tbody>
</table>

FUTURE CLOUD TRENDS
Despite these challenges, organisations have big plans for cloud over the next two years, with adoption and investment expected to grow. Almost all (92%) respondents state that over the next 48 months, their organisations will move infrastructure and workloads to the public cloud. Additionally, within two years’ time, respondents estimate that on average, almost a fifth (18%) of the IT budget will be spent on cloud technologies, rising from 12% today. The reliance on multiple cloud service providers will also continue to expand. Of the minority (33%) of respondents’ organisations that only use or plan to use a single cloud provider for IaaS, most (58%) are considering switching their approach to use multiple providers in the future. The message is clear: multi-cloud is here to stay.

CONCLUSION
More and more organisations look to harness the power of a multi-cloud approach, increasingly turning to cloud ahead of their own existing on-premises capabilities for IaaS consumption. Investment will continue to rise over the next two years and in that time more workloads will be migrated – embedding cloud into the very core of their operations and they will do so via multiple providers. However, is this multi-cloud approach currently leading to clarity (as it should) or complexity (as it could)? Data privacy and compliance, protection and resiliency are key areas for organisations working with cloud service providers but worrying, many may be inadvertently shifting too much accountability onto their cloud service providers. Organisations need to clearly understand their retained responsibilities in order to avoid the risks of noncompliance and cloud disruption that can have massive implications on their business. Doing so will allow them to properly access the benefits that a multi-cloud approach can offer.
White Paper

VERITAS RECOMMENDATIONS

As more companies embrace a cloud-first mentality, the need to navigate the complexities of a multi-cloud world is critical. As with on-premises environments, customers should consider all aspects of data management as they journey to the cloud, from data protection, compliance readiness, and workload portability to business continuity and storage optimisation. It’s important to keep in mind that adopting the multi-cloud can create environment fragmentation, so a unified approach to data management across on-premises and the multicloud is ideal. Another key aspect to a successful, long-term cloud strategy is to ensure flexibility and mobility of business applications and data, so organisations can benefit from all the multi-cloud has to offer without being locked-in to any one cloud. Veritas fully embraces a multi-cloud approach and is collaborating with many leading cloud service providers to help customers manage their data and extract maximum value from it, while helping to ensuring that no misconceptions abound regarding data management responsibilities. Veritas’ multi-cloud data management solutions can help organisations get to the cloud, from the cloud or between clouds with ease. We offer a wide range of solutions for data privacy and compliance, cloud migration, to and in cloud disaster recovery, storage optimisation, and backups and snapshots for data protection. Our holistic approach to managing data and applications across both on-premises environments and the multicloud is geared toward helping organisations be more competitive by attaining a digital-first footprint.

SCOPE AND METHODOLOGY

Veritas commissioned independent technology market research specialist Vanson Bourne to undertake the research on which this report is based. 1,200 senior IT and business decision makers from large private and public organisations in the US, Canada, UK, France, Germany, Switzerland, Australia, New Zealand, Brazil, China, Singapore, Japan and the Republic of Korea were interviewed in July to August 2017. All came from organisations that currently or planned to work with Infrastructure as a Service (IaaS) public cloud providers.

Interviews were conducted using a mixture of online and telephone interviewing. All were undertaken using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate. Unless otherwise indicated, the results discussed in this report are based on the total sample.

RESEARCH STUDY: KEY FINDINGS

- 76% stated “My organisation’s cloud provider takes care of all data privacy and compliance regulations.”
- 83% stated “My organisation’s cloud provider takes care of protecting our data in the cloud.”
- 54% stated “My organisation’s cloud provider takes care of secure transfer of data between on-premises and cloud.”
- 98% of respondents will move infrastructure and workloads to the public cloud.
- 58% of all organisations who just use one provider, want to switch their approach to multiple providers.

For more information, please contact CDW on 020 7791 6000 or info@uk.cdw.com