This research paper was conducted by IDG Connect on behalf of Sungard Availability Services. Targeting senior IT job titles in medium to large enterprises this paper focuses on Cloud Migration.

Cloud Workload Migration

Where the Cloud-Based Service Delivery Model Makes Sense
Summary of Research

A significant majority of applications and services remain in-house

- Within on-premises data centre/server farms
- Within off-premises, hosted cloud services
- Within other off-premises, outsourced services

Security tops concerns on the suitability of external cloud provider platforms for application and service hosting

Cloud services most suitable for business requirements

- Private (single-tenanted hosted)
- Hybrid (mixture of on-premises and hosted)
- Public (shared/multi-tenanted hosted)

Security: Myth vs. Reality

- %
  - Security
  - Reliability
  - Performance
  - Pricing and billing
  - Management

Migration Potential

Cloud Applications

Data Retrieval

Cloud Control

Single vs. Multiple Providers

Regulation

Interoperability

Conclusion
Enterprises Seeking Cloud Service Assurance

The cloud services market remains relatively immature but is forecast to grow significantly within the next five years in terms of both subscriber numbers and value. Enterprise IT departments have, to date, moved a limited number of specific applications, most commonly web applications (40%), office suites (25%), and CRM/ERP applications (23%) offered under a Software-as-a-Service (SaaS) model, out of their own data centres and server farms and into external cloud hosted environments.

But persistent concerns around the security (80%), reliability (37%), performance (28%) and management (20%) of cloud services means that the majority of physical and virtualised workloads (81%) remain anchored within on-premises infrastructure. Cloud-based security, backup and disaster recovery applications remain relatively underused by enterprise IT departments, for example, as do Infrastructure-as-a-Service (IaaS) platforms offering basic storage and CPU batch processing.

Widely reported, high profile outages which have adversely affected Amazon Web Services and Google in recent years have inevitably served to heighten enterprise mistrust of the cloud’s ability to provide the secure, robust application and service delivery that companies require. Yet the specific failure of public cloud services to isolate customer workloads and guarantee uptime do not tell the whole story: widely available alternative private and hybrid cloud delivery models based on dedicated, single-tenanted or like-minded enterprise-tenanted architecture hosted either off- or on-premises and connected by secure network links, can address lingering anxieties. In some cases, cloud service providers can demonstrate that they offer better physical security, data protection and failover capabilities than on-premises environments for example, whilst outsourcing responsibility for security to a third party can alleviate much, if not all, of the management burden associated with the constant requirement to configure and apply security patches and updates to the IT estate.

Many IT managers also worry that they will struggle to migrate and retrieve data quickly in line with national and European data protection regulations (37%), fears that can be addressed by hybrid cloud models that store important information on-premises and precise service level agreements which guarantee off-premises hosting arrangements comply with relevant laws.

Ultimately, it is the flexibility of the cloud services model which is a key attraction for many IT managers looking to spend less time on more routine operational tasks in order to place greater focus on improving overall business efficiency. Switching services into an on-demand, pay as you go model can improve server and storage utilisation, and depending on initial migration and set-up fees, offer better value for money than on-premises hardware provision in the long run.
Considerable Scope for Cloud Migration Exists

Most organisations still run a large majority of their IT applications, services and workloads within their own on-premises data centres (81%). This leaves significant scope to realise potential operational and efficiency improvements achievable by migrating some or more of those processes into external, off-premises managed hosting or cloud service environments.

Greater reductions in server and storage hardware/software installation, upgrade and maintenance costs, for example, are one potential benefit associated with pay as you go, or computing on demand services, that tie costs more closely to usage, compared to often low CPU utilisation rates associated with running on-premises systems. A study from research firm IDC conducted in 2012 found that moving on-premises hosted applications into cloud environments could save a company 70% on the total cost of ownership (TCO) associated with a single application over five years, though those costs will vary considerably according to the specific cloud service provider.

Indeed, IT staff routinely identify flexibility rather than cost savings as the bigger attraction of switching applications and services into a cloud-hosted model alongside the opportunity to free themselves from daily operational and infrastructure management tasks to focus on other projects by outsourcing the latter responsibilities to a third party.

Many, but not all, types of application are suitable for off-premises cloud provision for a variety of reasons however. Certain latency sensitive applications which demand responses in milliseconds, real time web applications with high performance demands or those with strict data security requirements may be better off either kept in-house, or hosted within hybrid cloud environments which tightly integrate, protect and secure dedicated, single tenanted off-premise and on-premise systems. However, given the potential benefits, companies should at least be analysing existing workloads to evaluate if and where operational efficiencies can be improved by switching to a cloud-based delivery model.

A significant majority of applications and services remain in-house

- Within on-premises data centre/server farms: 81%
- Within off-premises, hosted cloud services: 11%
- Within other off-premises, outsourced services: 8%
SaaS Leads the Way in Service Utilisation

Web applications and office suites (Google Docs and Microsoft Office365, for example) are the most commonly hosted cloud services, with customer relationship management (CRM), enterprise resource planning (ERP) and databases also popular forms of cloud-based SaaS delivery models being utilised. Storage and CPU batch processing are outsourced by only 16% and 5% of respondents respectively, indicating that IaaS platforms are relatively underused to date.

Whereas enterprise IT departments may be reluctant to trust mission critical workloads to public IaaS services delivered by Amazon Web Services, GoGrid and others, emerging private and hybrid IaaS platforms offering enhanced security, performance and network connectivity options from a range of providers should prompt a rethink in 2013 and beyond.

The message is similar for hosted security, and backup and disaster recovery services (currently used by 10% of respondents), where there is scope for third party providers to deliver more secure, high availability services than is often possible for companies relying on in-house resources alone. External cloud-based backup services store data off-site by default for example, often in multiple data centres adequately protected from power outages, floods and other events which allows for more robust disaster recovery options in the event of urban or regional emergencies. Many use centralised disk-based backups which utilise compression, encryption, and data de-duplication that stores and protects information more efficiently than equivalent tape-based operations and are able to backup data from multiple sites and offices simultaneously.

Potential customers must look to cloud service providers to give assurances, enshrined within appropriate service level agreements, that information is stored in compliance with local data protection regulations, that full recovery can be processed quickly and with little or no impact on production systems, and that there is adequate, secure network bandwidth between on-premises and hosted IT infrastructure to support the volume of data being backed up.

Cloud based IaaS and backup/disaster recovery services are underused
Data Security Concerns Holding Back Broader Service Adoption

Security remains by far the biggest source of concern for IT departments when it comes to selecting cloud service providers to host additional applications and services (cited by 80% of respondents) despite the fact that in many cases the cloud service provider’s ability to provide more effective data security is considerably greater than the resident IT department.

High profile outages which have affected the most widely used public cloud services in recent years have heightened ongoing security and performance concerns for many business customers. But both private hosted and on-premises, and hybrid cloud services using single-tenanted architecture and dedicated servers, storage and bandwidth can offer more robust protection than the shared multi-tenanted architecture characteristic of public cloud platforms which host different customers’ virtual workloads on the same systems simultaneously.

Various studies have concluded on-premises system security can be more vulnerable to malware, botnet and web application attacks than equivalent hosted systems for example, whilst in-house misconfiguration issues can also cause security problems. The gap between the level of security and reliability enabled by public cloud services and private/hybrid cloud alternatives tailored to more demanding enterprise customers presents a significant springboard for product differentiation and subsequent competitive advantage for providers, but only if they are able to educate potential customers and set out comprehensive service level agreements (SLAs) which guarantee data integrity for customers alongside uptime and application availability.

Maintaining effective data security protection through regular installation of application updates and patches also represents a significant drain on the IT department’s time which can be minimised by pushing that responsibility onto the cloud service provider.

The relatively small number of respondents (21%) highlighting price and billing as a concern indicates that compared to on-premises application and service hosting, and beyond initial set-up and migration expenses, cloud services are seen to offer either equal or better value for money by the majority of organisations despite costs varying significantly according to individual cloud service providers and specific workloads.

Security tops concerns on the suitability of external cloud provider platforms for application and service hosting
Customers Need to Know They Can Retrieve and Delete Data from Cloud Services Whenever Necessary

Of those surveyed, 37% remain uncertain (22% fifty-fifty, 15% not confident) that they can transfer data to and from cloud services quickly and easily and in accordance with European regulatory directives.

The overall findings indicate that confidence increases/decreases in line with the size of the organisation - 38% said they were very confident, but that number rose to 59% among companies employing over 20,000 people, suggesting that larger companies which have already outsourced greater volumes of information to third party hosting companies are more familiar with, and therefore less uncertain about, the processes involved.

Remaining concerns can be addressed to a certain extent via hybrid cloud platforms that store some data and legacy applications in hosted environments and others on-premises where data regulation or security and performance concerns demand it is hosted locally. They are also solved by SLAs and terms and conditions offered by some private-hosted and dedicated cloud services whose providers have sufficient data centre footprint of their own to guarantee that sensitive information stays either within its country of origin or the regional boundaries set out by data protection regulation, and can be quickly retrieved to meet the terms of subject access requests and eDisclosure directives for example.

Where data is hosted off-premises, terms that ensure any data returned to the customer is in a format which enables continued processing are crucial. Cloud service providers must be able to show that they delete all of the customer’s information when that customer terminates the contract and that no other copies are retained within their own cloud architecture, back up sets or the architecture owned by any subcontractor, partner or equipment supplier the cloud service provider may use. Efficient provisioning, migration, management and auditing controls are important here as are network connectivity and security mechanisms that guarantee adequate bandwidth and data integrity when information is being transmitted between sites.
Trust is Equal to Local Hosting and Application/Service Control

A reluctance to trust applications and services to fully hosted cloud services is highlighted by the type of deployment model in use, with these defined by the US National Institute of Standards and Technology (NIST). NIST sets out private cloud, defined as an infrastructure for the exclusive use of a single organisation either on-premises or off-premises; community cloud, provisioned for the exclusive use of a specific community or group of users which can again be either on-premises or off-premises; public cloud, a strictly off-premises system provisioned for the use of the general public; and hybrid cloud, an infrastructure platform composed of two or more of the previous three models integrated to enable data and application portability, to support cloud bursting or load balancing for example.

On-premises deployment models are preferred by the majority of respondents with private clouds rated of equal suitability (37%) to hybrid cloud platforms that integrate in-house with externally hosted systems. Private cloud services which are hosted on single tenant, or exclusive use, architecture within provider data centres were cited as suitable by only 13%, with public clouds attracting support from only 7% of the survey.

Respondents’ low support for public cloud services overall brushes over the suitability of shared, multi-tenanted architecture for some workloads but not others. In many cases the IT department will prefer to keep mission critical data and applications on-premises but can benefit from migrating others to flexible, pay as you go environments, including SaaS based office suites and Platform-as-a-Service (PaaS) providers to support software testing and development processes on a temporary basis to match on-demand requirements. The survey also delivered a strong indication that the vast majority of organisations are looking to maintain either total or partial control of any cloud service or application they may use, reinforcing the idea that the shared architecture characterised by public cloud services may not serve their needs.

Cloud services most suitable for business requirements

- Private (single-tenanted hosted) 37%
- Hybrid (mixture of on-premises and hosted) 7%
- Private (on-premises) 37%
- Public (shared/multi-tenanted hosted)
Cost, Performance and Reliability Benefits of Spreading Workloads Across Multiple Cloud Providers Largely Unrealised

The majority of organisations which have migrated cloud workloads to third parties tend to deal with a single service provider rather than designate different applications or services to multiple hosting sites, suggesting that many associate security, complexity and management concerns with maintaining and monitoring different cloud services simultaneously.

Where possible, customer workloads should be demonstrably interoperable and securely portable between virtualised environments which consist of different hypervisors, virtualisation platforms, operating systems, storage resources and network components, and allow migration without additional formatting of the workload to take place. There is scope here for third party providers and cloud brokers to address vendor/virtualisation platform lock-in fears and alleviate any provisioning and management burden by taking responsibility for the migration and monitoring of multiple workloads under a single managed contract backed by appropriate SLAs.

This provides the option of matching specific workloads into cloud services best placed to meet their requirements, such as cloud bursting CPU batch processing or temporary storage resources to support test and development cycles for example.

Various open source cloud management platforms and software stacks designed to simplify cloud-to-cloud and hosted cloud to on-premises (hybrid) cloud migration have recently emerged, notably the Apache distribution of Citrix’ CloudStack alongside that vendor’s own CloudPlatform derivative, the OpenStack framework originally created by Rackspace and the US National Aeronautics and Space Administration (NASA) agency, and the private cloud IaaS platform from Eucalyptus.

These aim to provide a solid basis of interoperability to rival better established proprietary platforms and service provider interoperability initiatives from VMware and Microsoft, though their success lies to a certain degree on the extent of support from multiple hardware/software vendors, cloud service providers and telecommunications carriers: i.e., their momentum is likely to increase according to the volume and breadth of cloud services between which virtualised workloads can be migrated.
UK and European Data Protection Rules have a Considerable Effect on Outsourcing Decisions

Organisations are storing large volumes of information that is subject to both UK and European data protection laws meaning they must pay close attention to how and where that data is stored and processed in the event of its migration to an external cloud service platform.

A business located in the UK for example is subject to the Data Protection Act 1998, which includes an obligation that the customer retains close control over its personal data, even when it is being processed by a third party on its behalf, and retains legal responsibility for that data's integrity.

Whilst EU law does not prohibit the transfer of personal data outside the European Economic Area (EEA), which includes all the countries in the European Union as well as Iceland, Liechtenstein and Norway, it does insist that there are adequate data protection safeguards in place before that processing takes place, unless the destination country has been pre-approved as having adequate data protection by the European Commission, including measures to ensure it is properly isolated and deleted when appropriate.

Any external cloud service provider trusted to handle company information must therefore be able to demonstrate adherence to any relevant data protection rules and provide visibility into security, storage and data retention processes, potentially allowing information security monitoring and audits and linking external hosted systems to on-premises platforms within broader hybrid cloud service delivery via secure network links such as virtual private networks (VPNs).

Companies should work closely with the provider to establish the exact details of service policies, processes and controls which determine how their personal data will be kept secure and establish safeguards to ensure information is stored in line with applicable laws.

A high percentage of stored data is subject to privacy legislation

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>80-100%</td>
<td>70%</td>
</tr>
<tr>
<td>60-80%</td>
<td>8%</td>
</tr>
<tr>
<td>40-60%</td>
<td>6%</td>
</tr>
<tr>
<td>20-40%</td>
<td>4%</td>
</tr>
<tr>
<td>Less than 20%</td>
<td>1%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>11%</td>
</tr>
</tbody>
</table>
Keys to Seamless Migration Between Multiple Cloud Providers and Services are Interoperability and Standardisation

Fast, secure and easy to manage cloud workload migration from physical to virtual servers and on-premises to hosted platforms, in the first instance, and between different cloud architectures, is imperative if organisations are to make optimum use of multiple hosted platforms, service providers, telecommunications carriers, consultancies and systems integrators to foster wider cloud service provision.

This makes interoperability assurances able to guarantee workload, application and information transfer without data loss, downtime or other adverse impacts to either off- or on-premises cloud infrastructure and broader business operations, all the more important.

End user confidence can to a certain extent be boosted by service provider adherence to standardised interoperability frameworks, best practice guidelines and other certification initiatives which make it easier for potential customers to compare and evaluate different cloud service offerings from the perspective of price, performance, reliability, security and SLAs.

Numerous examples pertaining to specific elements of cloud computing and service provision have either already been established, are being revised or are in development. But many remain relatively immature and, as with all standardisation and interoperability efforts, there is a genuine risk that initiatives will fragment rather than unify the market and confuse rather than reassure potential customers. These include the Distributed Management Task Force (DMTF) Open Virtualisation Format and the Institute of Electrical and Electronic Engineer (IEEE) P2301 and P2302 standards for VM migration, the Storage Networking Industry Association (SNIA) Cloud Data Management Interface for cloud-to-cloud storage interactions, and the Open Grid Forum’s Open Cloud Computing Interface which is building standardised network APIs to facilitate IaaS management.

Elsewhere, the Cloud Security Alliance (CSA) is focused on cloud service provider security certification, the Open Data Centre Alliance (ODCA) has defined enterprise-orientated cloud service usage models based on standardised multi-vendor platforms, and the UK-based Cloud Industry Forum (CIF) provides a code of practice for affiliated cloud service providers.

Cloud service standards and interoperability rated as very important by 79% of respondents

- Very important: 79%
- Important: 15%
- Not very important: 6%
Conclusion

The survey indicates there is significant headroom for enterprise IT departments to increase their use of cloud services and given the potential benefits associated with outsourcing a greater percentage of virtual workloads to a third party provider, they should at least be evaluating their remaining in-house applications and services to ascertain whether a switch to a cloud delivery model would make more sense from both financial and operational perspectives.

Security and data sovereignty fears are perhaps more prominent than they should be, and could be allayed by hosting applications and services in single-tenanted, off-premises private or hybrid cloud environments which tightly integrate external provision with on-premises systems. The delivery of customised contracts tailored to individual customer requirements and detailed service level agreements that clearly set out exactly how and where customer data is stored and protected in compliance with relevant UK and European Union privacy and data protection rules, alongside management, monitoring and control mechanisms that give customers complete visibility into cloud services so they can keep track of virtual workloads at all times, are also likely to engender that all important trust in the cloud provider.

Cloud service providers addressing the unique requirements of the enterprise market should pay close attention to the various currently underway. They are designed to make it easier to migrate virtual workloads from one platform to another and will provide another measure of reassurance for potential customers. The emerging open source cloud software stacks such as CloudStack and OpenStack should help here, especially as larger numbers of cloud service providers, hardware/software vendors and network providers lend their support. But cloud service providers should look to build on this potential to persuade a clearly sceptical audience that the seamless interoperability between cloud environments without disruption to production systems is achievable and desirable.

Opportunities for cloud providers to oversee and deliver managed services that utilise multiple cloud resources from different providers exist, but those looking to aggregate a mixture of Saas, IaaS and PaaS propositions under a single contract to handle cloud bursting or other on demand capacity boosts will have to work hard at proving their worth by augmenting them with efficient management controls and value added services for customers that will keep one eye fixed firmly on their own bottom line.