Fordway

Cloud Management

The C-suite guide to making cloud work for any organisation

www.fordway.com

Making cloud manageable

Executive summary

Organisations are increasingly turning to cloud to reduce the time and costs of managing their IT infrastructure and enable them to focus on their core business activities. The headline costs of public cloud services are falling, but before moving services it's vital to understand exactly what you are buying to ensure you obtain the service levels you require to avoid additional, unexpected costs. With some types of cloud service, you still have to retain responsibilities, skills and equipment in-house, while others may not be suitable for legacy applications.

To find the most appropriate mix of cloud services for your organisation, you need to begin with a review of your existing infrastructure and the services delivered over it. This will define the mix of commodity services and essential business applications your organisation requires, with their associated service levels. You can then make an informed decision on which services you ae best placed to continue to provide in-house, or under current arrangements, if any; which to move to cloud; and whether you would also like the cloud provider to manage the services on your behalf.

In many cases public cloud is a good option. If there is a good SaaS option available for the business applications or services you want to use, and costs are acceptable, it makes sense to use it. However, few of the current SaaS services available offer the ability to easily transfer legacy applications and all their associated data into them. If this is the case you will need to provide some aspects of the service yourself or use a managed cloud service which provides services using a defined and mandated process and to an agreed SLA. We explain what is included with different types of cloud service – PaaS, IaaS and SaaS, with and without management – and provide advice on how to evaluate managed cloud providers to ensure that you find the best fit for your business.

In Fordway's experience, medium to large enterprises with a small in-house IT team face the greatest challenges and hence have the most to gain from carefully chosen managed cloud services, which enable them to focus internal resources on the most business critical services.

Most organisations are likely to find themselves with a hybrid cloud solution, so we conclude by looking at the management and monitoring options available. Whatever service you choose, moving data to the cloud does not negate the need for an organisation to take proper data security precautions. You have to take responsibility for asking your chosen cloud provider to deliver the appropriate levels of information security and need to measure and audit them yourself to ensure that the relevant security is applied.

Fordway

Contents

Fordway's commitment to providing good quality independent advice has not changed in 26 years.

Our skills and expertise are applicable to any industry or market sector; our customers are defined by the size, complexity and importance of their IT operations rather than their industry.

Every organisation needs effective, efficient and optimised IT infrastructure, whether run internally, under contract with service providers or on the cloud.

For more information visit: www.fordway.com

or call us 08448 700100

Introduction

Whereas organisations once chose outsourcing to reduce the time and cost of managing their IT infrastructure, enabling them to focus on their core business, now they are turning to cloud. It offers the same headline benefits: transferring costs from Capex to Opex and freeing up in-house time and resources. It also has the benefits of limitless capacity, almost total flexibility and increased efficiency.

Whilst the headline costs of cloud services are falling, you still need to know exactly what you are buying to find the right solution for your organisation. Not all cloud services are created equal: with some, you still have to retain some responsibilities, skills and equipment in-house; others may not be suitable for legacy applications, so you are likely to end up with a hybrid solution.

It is vital to analyse your business needs and understand the characteristics of each application you propose to migrate before making any decisions. Once you have migrated, got rid of your in-house infrastructure and retrained and redeployed your staff, you have to use whatever the cloud provider gives you unless you migrate services again.

Migration between cloud services is not easy, particularly for complex applications. There are no simple methods of migrating between the major public cloud platforms – unless your applications are containerised, in which case they wouldn't be legacy applications! It is likely that you will require third party software and consultancy, further increasing cost and complexity. You also need to consider how to secure, patch and update cloud hosted applications, plus monitor and manage your providers to ensure that they deliver on the promised SLAs.

In this White Paper we begin by looking at how to define the services you need and their service levels. We then compare the different types of cloud to show exactly what is included with each service. Armed with this information, organisations can start to make informed choices on which services to move now, whether to wait until something suitable becomes available, or whether to remain with in-house provision and optimise their existing infrastructure in preparation for a future migration.

Getting ready for cloud

1. Review your existing infrastructure

Most organisations have unnecessarily complex IT infrastructures. This is normally because they have been built up through a series of perfectly valid but separate business decisions on core applications and services, all of which have ended up the responsibility of the IT team, without a clear plan. The end result is normally a complicated mix of broadly incompatible systems and services trying to be managed and supported as a common infrastructure. The integration issues and day to day management of these consumes a large amount of resource and cost while reducing resilience and providing little real business benefit.

One of the key reasons outsourcing failed to deliver on its promise was because services and infrastructure were simply transferred as they were, so the opportunity for improvement was missed. In the same way, simply transferring an existing service to cloud or a managed service provider without first reviewing its fitness for purpose and architecture will negate many of the potential benefits.

To cut through the complexity, the organisation needs to review its existing applications and services against the needs of the business – a business and IT alignment review. This will define the service levels required for the key operational processes that IT supports, with a full understanding of the cost, performance and availability implications of those service levels. Fordway has developed its own APAC methodology based on COBIT, which we have used successfully with a range of organisations; other frameworks for this are also available.

2. Decide what you want to do yourself, if anything!

After carrying out Step 1, your organisation will have defined a mix of commodity services and essential business applications, each with associated desired service levels. The next step is to consider how best to deliver them.

This requires a review of the current IT estate, including capability, capacity, age and maintainability of assets, plus a review of your data centre facilities, power provision and HVAC. If change or investment is needed, the next stage is to analyse what benefits a move to cloud could bring and what the business impact of such a change would be.

You also need to consider the application's likely usage patterns, and how fast it is likely to need to scale. All public cloud services are metered in some way; this can be both a good and bad thing, dependent on the application or service and its expected use.

For each service consider whether you want to provide:

- ownership of equipment
- skills, technical support and administration
- security
- monitoring and management.

Even if they run on someone else's cloud, you will almost certainly manage, maintain and update the business applications yourself, but there may be other, simpler services, such as file storage and email that you choose to hand to a third party. This could be because:

- high quality and cost effective SaaS options for these services exist
- they are non-core or commodity services
- you do not have the skills in-house or cannot justify the cost of employing specialists to support them e.g. a storage and back-up management, security
- Aspects of your existing infrastructure are reaching end of life.

3. Compare different types of cloud

Each type of cloud includes different levels of service and management. As well as considering security responsibilities, you need to consider who will be managing your cloud services. Do you simply want a third party to provide capacity and equipment, or would you like them to be able to handle the management too?

Infrastructure as a Service (IaaS) is basically re-platforming an existing application onto another provider's infrastructure. With public cloud IaaS you simply get the hosted VM; all other elements, including patching, backup, security, resilience and the application support and management inside the instance are up to you.

Platform as a Service (PaaS) provides a base application, such as a database, development or runtime environment, which is secured and patched, onto which you put the application or your code. You still have to maintain these elements.

Software as a Service (SaaS) should provide a fully managed, patched, secured, updated and resilient environment that you just use.

These cloud options come with different levels of security included, which is outlined in Table 1.

	Service provider security responsibilities	Customer security responsibilities
IaaS	Control access to the hosted instance, good general security up to and including host and hypervisor patching and proactive infrastructure security monitoring	Securing access to the instance(s) and everything inside them, plus security of integration between instances unless you contract the provider or other third party to do it for you
PaaS	All the above plus OS and platform patching	Access and authentication to the service plus application and code patching for any service running on the platform
SaaS	Overall security of the service, including responsibility for securing any client data hosted within the service	Authentication to the service and data transfer between service providers

Table1: Security responsibilities for different cloud services

4. Considerations for legacy services

Moving applications such as your corporate email service to a public cloud SaaS service is straightforward. The challenge comes in moving applications which may have been originally developed ten or more years ago and on which the business relies. These could be bespoke applications developed in-house, or specialist packaged applications which have been customised to organisational needs and where the software providers' SaaS offering, if available, cannot accept the customisations. Few of the cloud services currently available offer the ability to easily transfer legacy applications and all the associated data onto them.

In this instance the options available are:

Cloud re-platforming onto IaaS, where you retain existing licences and support with the application provider. You are still responsible for patching, resilience, back-up, security and application support and maintenance of the application(s) in the VMs (see Table 1), as well as monitoring and management.

Managed IaaS, offered by Fordway and other suppliers, where the monitoring, management and maintenance services are included, plus normally a manned Service Desk and the opportunity to define custom SLAs.

PaaS, where the cloud provider provides a secured and patched base application, such as a database, development or runtime environment, onto which you install and manage your own tailored application or code and retain responsibility for maintaining the application itself.

- Most legacy applications will need redevelopment to work on publicly available PaaS services, as these are generally based on the current versions; there are not many SQL Server 2008, Informix or Progress DB PaaS services. If this does not make business sense, moving to a suitable IaaS is pretty much the only option.

SaaS, in which responsibility for all aspects of the application are transferred to a third party provider or partner. If available, you or the provider can customise the service to the exact characteristics required, providing a tailored service while enabling you to take advantage of cloud's low costs, scalability and flexibility.

- This normally requires either significant customisation of the SaaS offering or accepting that you can work without your customisations and enhancements.

So a cloud solution is achievable, but you will probably need to use private cloud or managed IaaS as a staging point until more appropriate public cloud services become available.

5. Considerations for managed services

As mentioned earlier, one of the considerations is whether you want your cloud provider to include management – for example managed IaaS or SaaS. One of the benefits of managed cloud is the cost effective delivery of high quality, fit for purpose and guaranteed service levels that meet or exceed those your organisation requires. The following is a checklist to consider when evaluating potential managed cloud providers.

SLA

We recommend that as well as including service levels the SLA includes several other factors which we believe are vital in the relationship between organisation and service provider:

- accountability
- service monitoring and management
- a regular communication programme, including regularly scheduled Service Reviews and meaningful reporting mechanisms.

Responsiveness and flexibility

Challenges will arise in every relationship due to changing requirements or organisational afterthoughts, and the end user expects and deserves a rapid response to these dynamic situations. Unexpected developments or contingencies will always surface, even in the best of relationships. When these challenges become points of contention, a natural reaction for each party is to build its own encampments — the service provider around the statement of work (SOW) and the end user around the service level agreement (SLA). Neither of these knee-jerk reactions is particularly productive in solving these challenges. The more responsive and productive approach is for the service provider to help the client recognise possible changes in requirements in a timely fashion.

Culture

Do you like the people you will be dealing with and do you feel that they care about your business? If your business changes you will need to change the terms and conditions appropriately, but if there is a large amount of legal jargon wrapped around every sentence of the contract, and every discussion refers back to these or the contract, are you sure they have your best interests at heart?

Two aspects that can deter organisations from considering managed cloud services are a perceived loss of control of network and services and concerns about trust, reliability, security and continuity. Any organisation which chooses to go down the managed cloud service route should expect at least as much commitment, probably more, from their service provider as they would have obtained from their in-house team.

6. Cloud management and monitoring

6.1 Cloud Management

An effective management service pulls together service availability and other performance information. It should have the ability to carry out synthetic transactions against defined services and applications, show overall system health and monitor response times and latency.

Management might be perceived as superfluous for cloud services, as they are designed to be commodity services, primarily with user self-service through web portals. However, most organisations prefer, and in many cases need, a human voice and face plus organisation specific information from their services. Additionally, particularly if you are using SaaS services, there may be several providers who collectively provide your IT service, and you will need both visibility and common incident and problem management across them.

Cloud management services provide service integration, management and monitoring for all cloud services contracted by an organisation. They offer major incident and problem management, with escalation to third parties if required, and may also include asset management of devices and infrastructure. The features to look for in a third party cloud management service include:

- customisable services and reporting
- cross supplier service consolidation and reporting against defined service levels
- independent review and reporting on third party supplier performance
- service on-boarding and service management for multiple partners
- the ability to work with other organisations e.g. network providers for WAN links
- 24 x 7 monitoring and support.

An engineering joint venture was set up by three large organisations to deliver a major infrastructure project, and they decided to create an independent IT infrastructure and outsource management to a third party. By using a managed service they were able to get the infrastructure up and running quickly and ensure consistent access for all parties. They can add capacity as and when needed, only paying for the capacity used, and then scale it back as the project draws to a close. They also have the security of knowing at the end of the contract they will have no residual issues and the environment will be torn down, with the data distributed as required. This type of framework is ideal for "volatile" projects, providing IT on a pay as you need basis.

6.2 Cloud monitoring

Monitoring requires an audit function to ensure that the services are and remain fit for purpose. Organisations whose IT service is now dependent on multiple cloud and other external suppliers will want to know:

- how well are my service providers performing against contractually agreed SLAs?
- if they are not performing, where is the problem? This is particularly important where multiple providers are responsible for elements of the IT service
- is the aggregated service delivering suitable performance to our user community?

This is leading to a growth in Cloud Monitoring as a Service (CMaaS) to monitor the performance of multiple suppliers, all of whom will claim 'it's not their fault' when a problem arises if they believe they can get away with it. These services provide organisations with full visibility of how well each individual provider and the overall IT service are performing.

6.3 Cloud security monitoring and management

Moving data to the cloud does not negate the need for an organisation to take proper data security precautions. You have to take responsibility for asking your chosen cloud provider to deliver the appropriate levels of information security and need to measure and audit them yourself to ensure that the relevant security is applied. Particularly with IaaS, less so with PaaS and SaaS, you also retain a number of security responsibilities and, irrespective of who hosts the data, under both the Data Protection Act and the forthcoming GDPR legislation you are responsible for your data and its security.

Before moving any data to the cloud, ask your potential service provider:

- Who is the ultimate holder of the data?
- Where is the data held?
- Do you operate good processes and can you prove it?
- What specific security standards and levels of security are you applying to my data?
- How can you guarantee that no-one else can get access to my data unless I specifically want them to?

Organisations should check all this information for themselves and manage it as they would for every corporate risk.

An organisation was not large enough to have its own network security expert, so this role was handled by the senior IT technician. In response to a security attack, he disabled a number of ports/access methods on the firewall and external routers. However, he did not fully comprehend the implications of the settings entered, to the extent that he cut off all customer and external access to the organisation for 48 hours, with commensurate negative impact on the business. An external organisation with the appropriate skills can quickly implement changes such as this without any unwanted consequences.

Conclusion

In many cases public cloud is a good option. If there is an appropriate SaaS offering available at an acceptable price it makes sense to use it. However, many providers are currently offering something that is more like PaaS, so you will need to provide some aspects of the service yourself, or use a managed cloud service.

Managed cloud services offer significant business benefits by enabling organisations to focus on the IT activities that add value to their business while saving money and improving productivity. They provide specified services, with a defined and mandated process and to an agreed SLA. Managed cloud services also help organisations to manage skills shortages by using the skills of the service provider to complement those they have in-house.

There are many different ways to provide managed cloud services, and what is right for one organisation may not suit another. However, we believe organisations are missing out on a significant potential for cost savings and increased efficiencies if they do not consider the opportunity managed cloud services offer when reviewing their IT infrastructure provision.

In Fordway's experience, medium to large enterprises face the greatest challenges in funding their IT infrastructure. With a small in-house team, they are unlikely to have the diverse range of skills required to run a complex IT infrastructure, and hence either have to take a 'best guess' approach or turn to external experts on a regular basis. Carefully chosen use of managed cloud services will enable them to focus internal resources on the most business critical services.