

Fordway

IT Services. Excellence delivered.

WHITE PAPER

YOUR ROADMAP THROUGH THE CLOUD

www.fordway.com

Executive Summary

For most organisations the question is no longer whether it is appropriate to adopt cloud, but when is the right time and what services to move?

Moving one or more services to cloud is a strategic decision, but as with any change programme it is just the first step in a journey, and can be approached in many ways. This is particularly true for organisations which currently provide the majority of their IT services in-house. In addition to the technology change, migrating to cloud puts more emphasis on two key factors needed to deliver successful change: people and processes. When these, along with vision, have been addressed, the actual technology decision becomes straightforward.

Here we outline how organisations can go about planning, transitioning to and managing their IT services when migrating services partly or wholly to cloud. We also look at the key considerations to ensure that cloud provision can be switched between different suppliers in the future.

Contents

1. Essentials for the cloud journey	3
2. Mapping the journey	7
3. Questions for potential suppliers	10
4. Migration	12
5. Supplier management	13
6. Managing hybrid cloud	13
7. Fordway's cloud intermediation services	14
Conclusion	14

1. Essentials for the cloud journey: vision, people, process and platform

When considering cloud the key questions are: when is the right time and what services to move? Any change in IT services is usually driven by a 'compelling event', i.e. something that requires you to rethink what you currently do and to take action. This could be anything from the need to upgrade key applications to replacing core infrastructure or relocating a data centre. Cloud should certainly be one of the options to review. This is complicated in that there are many types and flavours of cloud; which ones should you consider? Some are likely to make more sense than others, and each has cost, compatibility, service availability and security issues to assess along with other business risks.

Moving data to the cloud does not negate the need for an organisation to take proper data security precautions, and the varying cloud options come with different levels of included security. Very simplistically you should expect the following from each level:

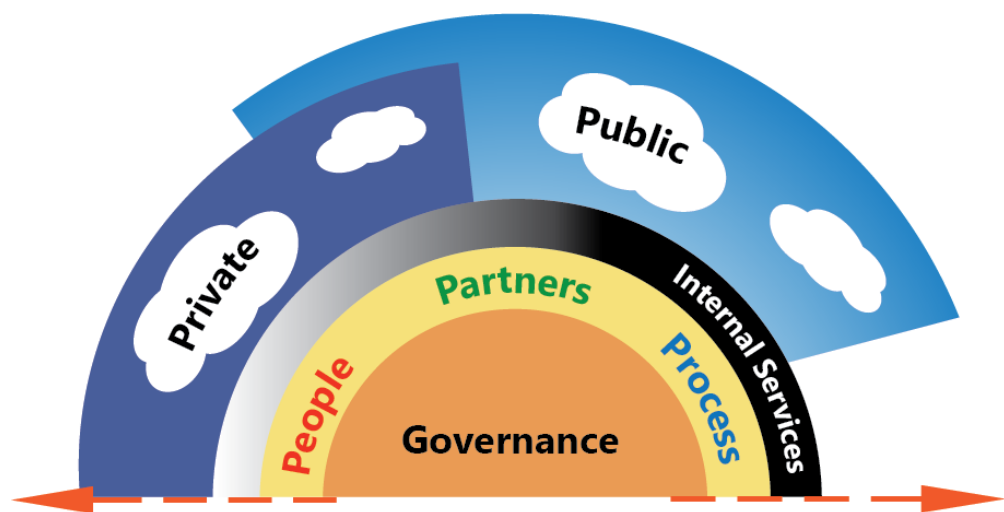
	Service provider security responsibilities	Customer security responsibilities
IaaS	Control access to the hosted instance, good general security up to and including host and hypervisor patching and proactive infrastructure security monitoring	Securing access to the instance(s) and everything inside them plus security of integration between instances or 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

Should you decide that cloud is appropriate, it is in effect another infrastructure migration project. If you currently run the impacted IT services in-house, however, your staff may well believe that their jobs are at risk. This, together with the perceived risks of moving to cloud, can make the migration three times as long and several times as complicated as it needs to be. In our view there are four requirements for a successful move.

1.1 Vision

The first stage of any project or programme is to craft and communicate a vision for the future that is clear to all stakeholders, which they can commit to while understanding what it will mean to them. This vision needs to provide the compelling reason for the project to go ahead, such as a move to new premises, a need to refresh existing infrastructure, the end of an outsourcing contract or a major organisational change.

Fordway has completed over 200 major IT infrastructure transformation and cloud migration projects for a wide range of customers across public, private and not-for-profit sectors in the last five years, and we have contributed skills and expertise to hundreds more. The vast majority have achieved the expected benefits or savings. When we analyse projects where the desired outcomes were not achieved, in many cases the reason was that stakeholders had misaligned or even conflicting expectations of what a successful outcome would be. Setting and communicating the vision for change, and defining what success looks like and how it will be realised, are the most fundamental factors defining whether the project will be judged a success or failure.



1.2 People

As part of crafting the vision there should be communication with your staff and other stakeholders to ensure they understand what it means for them. It is vital to get people on board throughout the organisation. This includes commitment from the top and support from the team at the coal face.

Change is always difficult, and particularly with cloud, as staff will be worried that their jobs are at risk so may not fully commit to the project. If people are to support the change, there has to be something in it for them. This generally means job security, new skills and hopefully recognition and increased salary. It is also possible that there are team members for whom the project does not offer anything. If this is the case managers should address it at the start of the process so it does not adversely impact the project at a later stage.

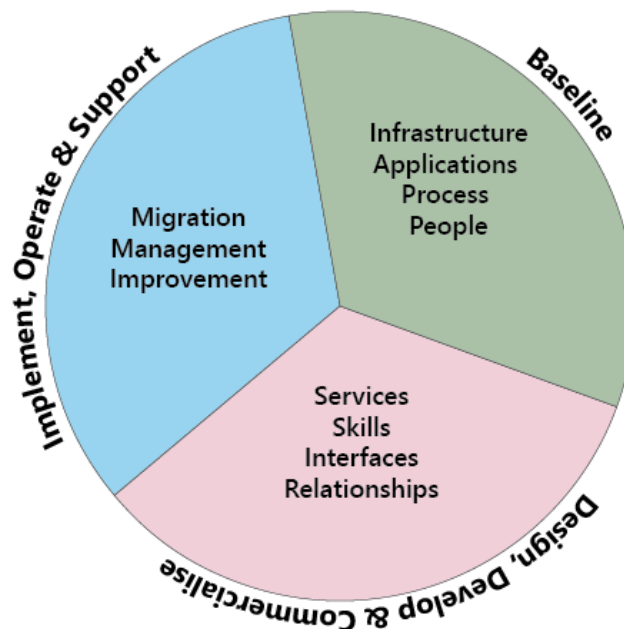
A key part of this process is consultation. You will need to interview IT staff who would potentially be impacted by a move to cloud in order to gain a full understanding of their attitude and capabilities. The SFIA provides an excellent model for IT staff alignment which will help in assessing existing and required

capabilities, and defining what is needed to develop and retain staff to meet the future vision. Once someone's future career plan is discussed and agreed it takes away considerable anxiety and builds trust, which improves performance. This approach also significantly reduces project and operational risk.

Communication is vital. Too much is never enough, as staff and other stakeholders will naturally assume the worst when there is silence. Keep them informed throughout the change process.

1.3 Processes

Organisations need to align their processes with those of their chosen cloud provider/s, as it is unlikely that a provider will change its processes to suit a customer.



One of the key characteristics of cloud is that it provides standardised, commodity services that are used in a standard fashion by means of standard processes. AWS, Azure, Google and all the other major public cloud providers have defined, standard processes, which is one of the major benefits of cloud and a major factor in its cost effectiveness. Unless you are a government or a multibillion pound corporation, you are unlikely to be able to persuade them to revise their processes, architecture or standards to suit your organisation. It is also possible that integrating their processes will help your organisation's IT service become more responsive and flexible, which is never a bad thing. If you need the flexibility for the provider to adapt its processes to suit you, you will be better off talking to private and virtual private cloud providers rather than using public cloud.

The best way to address how to map your current processes with potential cloud providers is to carry out a business and IT alignment review. This ensures that your organisation fully understands its capabilities (start point) and strategic goals (end point) and has accurately defined the service levels required for the key operational processes that IT supports. The organisation also needs to understand how it currently delivers services and what improvements it would like to make, and have clarity of the cost, performance and availability implications.

We find that many organisations operate their IT without defined and agreed service levels (SLA), or have defined service levels but no way of measuring them to ensure they are being met. Whilst many IT teams have concerns over committing to service levels, in our view they have a number of positives. Firstly, by defining SLAs and explaining what they mean, you are setting expectations for the user community you are serving. Secondly, they allow you to align service cost to the SLA. A service that has an SLA of 99.5% measured annually (i.e. allowing up to 43 hours downtime per year) needs considerably less resilience and is therefore considerably less expensive to operate and support than a service with an SLA of 99.95%, measured monthly, which allows a maximum of 21 minutes downtime per month.

Once an organisation has defined the services it needs, it can then decide which of them can usefully be provided via cloud and which to retain in-house, before aligning the selected services with the chosen service provider(s).

In the main most cloud providers follow ITIL processes and offer user self-service for some or all elements of the service, so it is likely that most organisations' existing incident processes can easily be adapted. Change is often through user self-service, so is usually easier to do, but for metered services even minor, incidental change often carries cost implications.

1.4 Platform

The final stage is to choose the most appropriate platform. If the preparation has been carried out correctly, the choice of platform is almost immaterial, as these days almost all the technology is pretty good.

2. Mapping the Journey

Planning the transition to cloud is the same as for any other major change: analyse, design, transform and operate. Each organisation will choose different parameters, which could be the quickest route, the most cost efficient manner, to fit with other corporate milestones etc.

2.1 Analyse

The initial step is to clarify the vision, as discussed in section 1, and then to analyse and audit where the organisation in terms of people and process. This stage includes a review of the current estate and the services delivered, why and what benefits the change or migration could bring and what the business impact will be. This will help define the proposed strategy for each element (e.g. migrate to virtual DC as is, replace, upgrade then migrate, migrate to SaaS service etc.), the data and operational security requirements/classification of each element and the technical and integration requirements for each.

A key question is how much work the organisation wants to do following a move to cloud?

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

Platform as a Service (PaaS) provides a base application, such as a database or development environment, which is secured and patched, onto which you put the application or your code, but these elements still require maintenance.

Software as a Service (SaaS) should provide a fully managed, patched, secured, updated and resilient environment that you just use. Many organisations choose to retain core business applications in-house, but move non-core or commodity services to the cloud. Most want to hand over responsibility for areas where they do not have the skills in-house or cannot justify the cost of employing specialists.

For most organisations, the optimum solution will be a hybrid of public cloud, managed cloud and in-house service provision or private cloud. Products such as Salesforce, Google Apps and Microsoft 365 integrated into corporate desktops can be considered as hybrid cloud, but they provide point applications and services only. Hybrid cloud is likely to be a staging point as organisations continue their cloud journey and services become more capable and resilient.

2.2 Cloud First Strategy for Disaster Recovery

Organisations looking to extend the life of their existing infrastructure should consider the strategic benefit of moving their Disaster Recovery to the Cloud, which can be a very useful first step in your cloud migration journey. There are three key benefits to this:

1. It gives you a first step to using cloud at a lower risk than moving your production environment into it. This option provides the opportunity to thoroughly test systems and learn about the appropriateness of services for the cloud without having to compromise service delivery.
2. By consolidating your passive DR environment into your existing production infrastructure you get more capacity and potentially a longer life for your current systems.
3. When the environment is set up and tested your costs are significantly reduced. Both AWS and Azure offer on demand services which allow you to stop virtual machines, so you don't need to pay for them, you only pay only for your data storage (plus any replication costs) until you fail over. This means that you only pay for what you use and when you use it.

2.3 Design

When the analysis has been completed, and a decision about which services can be moved to which type of service has been made, the next step is to size and secure the chosen cloud services, taking into consideration the required agility and elasticity i.e. 'just in time' provisioning, utilisation charging and burst capabilities. This is an opportunity to identify consolidation opportunities, enabling costs to be cut by reducing the number of environments to license, patch and manage.

It is also a good time to review policies. Do you need a test and development environment available 24 x 7 x 365? Most in-house services run this as most organisations own the hardware and datacentres the services run from, so the incremental cost saving of turning them off is small. However, with cloud services that are billed by the hour, minute or even metered usage such as CPU cycles or data ingress and egress costs can mount. If you can shut down the services for the 60% of the week that they are not needed it provides a considerable cost saving.

Services need to be imaged and architected so that they can be suspended or shut down, and then resume operation quickly in the state before it was suspended. Planning and assessment tools can assist by collecting environment statistics and performance metrics from existing systems, which can then be used as the basis for making operational decisions on how the environments can best be managed to minimise cloud expenditure.

Services should be mapped against resilience and availability to allow the appropriate configuration of cloud services to meet the required system Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) to deliver the organisations' business continuity requirements. Disaster Recovery requirements may be provided within the IaaS/PaaS supplier services through data replication across multiple domains, or with IaaS and PaaS service or environment replication to a separate cloud provider, depending on requirements. SaaS services should be natively resilient; this is an issue to address with the provider as part of the service selection criteria.

The design should provide the flexibility to enable organisations to adopt different platforms or alternative cloud suppliers quickly and with minimum impact to existing services. This ensures that they do not simply swap one legacy infrastructure for another.

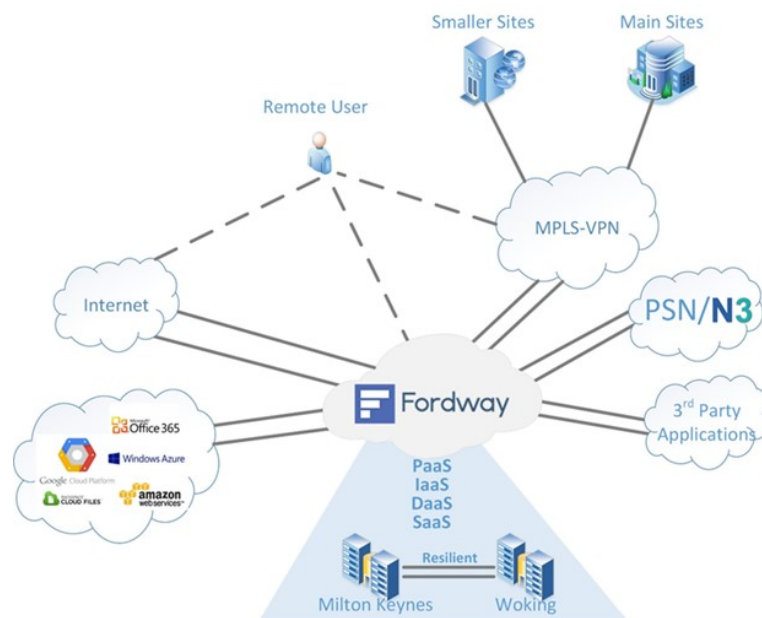


Figure 2: Example of Fordway hybrid cloud service

To manage cloud effectively there need to be clear definitions and ownership of the boundaries of the service levels. IaaS is the base layer of any service. It then needs to communicate with the OS, middleware and service layer (PaaS) to communicate with the application logic and interface (SaaS). These definitions should address computer power, operating system, server roles and their associated configurations, middleware such as JBOSS, BizTalk, SQL or Sharepoint, applications and interfaces, as well as responsibilities for testing and implementation of patching and supplier interdependencies.

Whichever combination of cloud services is chosen, the organisation still needs to retain responsibility for ensuring that the cloud provider/s meets the agreed SLAs.

There are a multitude of cloud providers, with significant differences in their contractual terms and conditions, available SLAs and recompense if not met as well as the legal jurisdictions where data is held and data recovery terms. Remember, this is where corporate data will be held to provide services which are fundamental to business operations. These will be important considerations when ensuring your services are GDPR (General Data Protection Regulation) compliant.

It is also important to make sure that the interfaces used are as standard as possible e.g. XML, SOAP, REST, SAML, S3 etc. It is worth noting that standards, unless they are their own proprietary ones, are rarely in a vendor's best interests. Smaller vendors may be better at developing services with standard interfaces as they have less market power to 'enforce' compliance with their own standards. Unless you want to be locked into a particular vendor's walled garden it may be better to choose services from challenger vendors, rather than from the very large vendors who often use proprietary interfaces.

3. Questions for potential suppliers

To help in modelling cloud services to enable evaluation and comparison between different suppliers, we have developed a checklist of key issues to consider.

Persistent (reserved), non-persistent (on demand) or metered instances – is the service required 24 x 7 x 365? If not, what do you need, and can the provider deliver this effectively? It doesn't happen very often, but AWS' terms and conditions allow them to shut down on-demand instances without any reference to the client. Does what you are contracting for offer the level of availability needed and which provider's model gives a more cost effective provision? Are there specific times that the service must be available and will the provider ensure these within a non-persistent service? Under metered services what guarantees will the provider give that all capacity is available even if not used? What actually constitutes usage? Several applications generate keep-alive packets to ensure availability, and these can be used by providers offering metered instances as the basis for charging even when services aren't actually being used.

Optimisation - will general purpose instances suffice or are computer, memory or storage optimised instances needed? Costs for these vary dramatically, both from individual suppliers and between providers. This goes back to really understanding the characteristics of the service being migrated onto the cloud platform.

Granularity of the charging model - what is actually included or is everything an extra? If an extra, how is it charged and what is the likely impact on the overall charges?

What is the security classification/business impact level of the data within the service? Does this mandate physical location awareness, and if so where will the organisation's data be stored? What security, access, audit and compliance controls need to be in place and can the provider guarantee them? If so, how – self certification or independent testing and validation?

What are the standard levels of resilience offered? Do they meet the organisation's requirements? If not what additional resilience is available and what are the costs? What service guarantees are offered and does the provider offer credits or other compensation if these are not met? If so, is the compensation worthwhile?

Service resilience - does the organisation want both primary and recovery services, where applicable, hosted by the same supplier? Do you have or need an independent backup to restore from in extremis?

Contractual and commercial relationship - what level of flexibility is offered? Are there any exit or data transfer costs should the organisation wish to switch suppliers? Is it an open ended contract or for a specified period? Under what terms?

Operational management of the service – is it all via a portal? If so, how does the supplier handle escalation and service updates? What processes does the supplier use for Problem Management or Major Incident Management, and do they have SLAs?

Operational process integration – does the way the supplier operates fit the way the organisation needs to operate, and if not is one party prepared or able to change to meet the other? What are the cost and impact of making those changes, and do they provide business improvement or provide cost savings over the contract term?

Cultural fit – this may seem trivial but does the provider's mission and values reflect those of the customer and other providers being managed under the agreement? The organisation is potentially entering into a multi-year agreement which will impact the services it offers its end users and it helps to ensure that all parties are aligned before committing to any agreements.

Security standards – does the potential supplier adhere to recognised security standards and can they prove they have the relevant controls in place? If not, how will they guarantee that their infrastructure is secure and patching is up to date? Organisations which have to meet public sector requirements such as PSN, for example, will be regularly audited and tested by independent external providers to ensure that they meet the latest security standards and have tested and audited procedures for dealing with any security incidents that may occur

4. Migration

Once the design phase has addressed all the potential issues and the new environment design has been approved, the next challenge is realising the Vision: how do we get from here to there? Ideally this will be without any business interruption and as part of a seamless transition, after which your user community will congratulate you for making their lives easier, happier and more productive.

Unless the migration is incidental and of little business importance, planning and project management are key. Migration to cloud is still an infrastructure or application migration; as a minimum it may involve data migration to a new application with a short period of parallel running. For one of our clients it involved physically and logically migrating 800 servers with associated applications, integration and dependencies into a new environment and upgrading and rebuilding the environments into a new security model without any service interruption, all to a key date that could not slip or the potential liabilities ran to many millions of pounds. We completed it successfully, in co-ordination with four other suppliers, before the due date.

Whilst Agile is all the rage, we recommend for migrations of this type 'traditional' project management such as PRINCE2, which give the framework and controls needed. Sprints are good for smaller work packages, but they need to be aligned to the overall plan. As with all successful change projects, you need to get your people aligned and prepared, give them clear guidance and manage the exceptions that will undoubtedly occur.

5. Supplier management

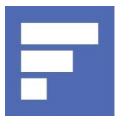
Once an organisation has moved one or more services to cloud, it still needs to actively manage its cloud portfolio and monitor performance against SLAs. This is leading to a growth in new services (Cloud Monitoring as a Service, or CMaaS) to monitor the performance across the multiple suppliers who will now be interdependent, and critical, to your IT Service Delivery and to your user community. Should a problem arise, their default reaction will either be 'it's not our fault', or more invidiously 'prove it's our fault'. Suitably configured CMaaS services provide you the ability to see where issues are, and whose responsibility it appears they should be.

It is vital that these services are independent of the providers themselves, but that the providers either provide visibility into their service or you can contractually ensure that they do. Such services should consolidate events and other performance statistics across the IT supply chain, showing overall service health and providing the ability to drill down into specific services where required. An added service, Security Monitoring as a Service (SMaaS), is equally important. This can run alongside or be integrated with CMaaS to ensure that core services are secure as well as available.

When choosing such services, look for integration with public cloud services (e.g. Office 365, Salesforce, Huddle, Google Apps), IaaS and PaaS services (e.g. Microsoft Azure, Amazon Web Services and Google's App Engine). Some services such as Fordway's CMaaS can carry out this this monitoring from a single pane of glass and can also be used to monitor traditional IT services such as in-house environments, plus hosted and private cloud services where agents can be deployed or gateways installed into the monitored environment. Network monitoring is provided as part of CMaaS, with the results integrated into event correlation which are displayed on custom HTML5 dashboards, allowing for policy-based SLA measurement of hybrid cloud environments across multiple suppliers.

6. Managing hybrid cloud

Cloud management might, on first thought, be perceived as something that is not required for cloud services, as they are all 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, there may be several cloud providers who collectively provide your IT service.



7. Fordway's Cloud Intermediation Services

Choosing the right mix of cloud services and the most appropriate provider/s can be a complex series of decisions. To assist in the process Fordway offers a range of cloud intermediation services. These cover assessing an organisation's IT Service Delivery capabilities and strategy, helping it realign to operate in the cloud, advising on the most effective hybrid cloud model for current and future needs, and assistance with implementation, support and operations. Our experience in defining and negotiating such contracts enables us to ensure that the deliverables from the cloud provider are well defined, fit for purpose and optimal for your organisation.

As well as these consultancy services, Fordway is also a managed cloud provider offering a wide range of services, including PaaS, IaaS, SaaS and more specialised services such as patch management (PMaaS), identity management (IDAMS), plus the cloud monitoring, security monitoring and cloud management tools to enable organisations to monitor their cloud environment. These are provided from our two UK Tier 3 data centres.

This combination of skills makes us uniquely qualified to help organisations choose the best cloud solution for their needs. As a provider ourselves, we know the right questions to ask to ensure that organisations get what they need from their suppliers, and that services are portable and future-proof. We do not hesitate to recommend public cloud where it provides the most appropriate solution, but will ensure that costs and service levels are thoroughly analysed to avoid unexpected bills. We can host more difficult or legacy services that are not currently suitable for public cloud, or need a higher level of security than can be guaranteed on public cloud. This hosting can either be an interim solution until a replacement application is developed, or a more permanent answer should public cloud not be the most appropriate option.

Conclusion

Moving to cloud is a more complex transition than other infrastructure change projects, particularly if most of an organisation's IT services are currently provided in-house. As with all change, the key to delivering it effectively is to understand what you want to achieve and why, build alignment across all the people involved and, with cloud, to get a full understanding of the costs and implications of the migration before you do it. Whilst it isn't easy, good things never are, and by following a planned process cloud can provide significant benefits to your business operations.

For more information visit www.fordway.com
or call 08448 700100