Fordway

Cloud Roadmap

A Guide to Planning and Managing the Journey to Cloud

www.fordway.com

Fordway

Introduction

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.

In this white paper 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, and how to manage and secure your IT services once they are distributed across multiple suppliers and locations.

1. Essentials for the Cloud Journey: Vision, People, Process & Platform

When considering cloud, a key question is when is the right time and what services to move. Generally, any significant change to an organisation's IT services is 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 This could be anything from the need to upgrade key applications, replacing outdated infrastructure or relocating a data centre. These days, we recommend cloud should be one of the options to consider. This is complicated in that there are many types and flavours of cloud; which one(s) 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:

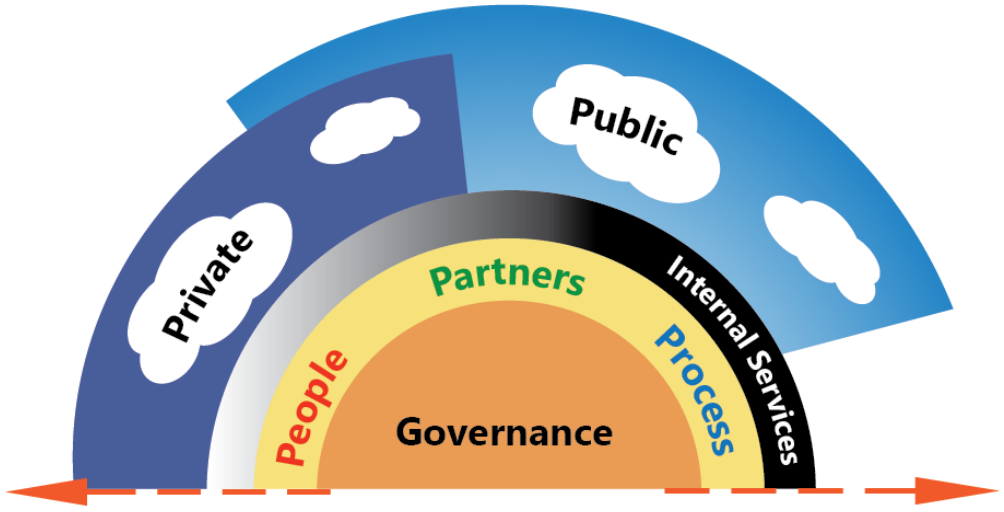
	Service provider security responsibilities	Customer security responsibilities
IaaS	Control access to the hosted instance, good general security up to and including host and hypervisor patching and proactive infrastructure security monitoring.	Securing access to the instance(s) and everything inside them 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 – with the further complication that if you currently run the impacted IT services in-house, cloud can be seen as another form of outsourcing, so 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 considerably longer 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. Unsurprisingly, not every project has gone exactly to plan, thankfully 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 some of the most fundamental reasons 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 going to support the change, there has to be something in it for them, which 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 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 your IT team's 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 and also significantly reduces project and operational risk.

Communication is also 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. 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 first 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 their cost, performance and availability requirements and their 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 needed, 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).

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, such as public cloud IaaS and PaaS services, please be aware even minor incidental change often has cost implications.

1.4 Platform

The final stage of any successful change 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.

We have looked at all the leading public cloud services and all are very capable, although the range of complementary services and the providers' billing models vary. It is important to check the small print, particularly the terms and SLAs offered, and organisations need to monitor performance against the SLAs themselves to ensure they receive the contracted service. Some legacy or bespoke services, or those which require a non-standard SLA, may be difficult to transfer to a public cloud service, so retaining them in house or working with a virtual private cloud provider will be the better option. However, these can still potentially be managed from a single point (see section 6). The choice of platform is discussed in the next section.

2. Mapping the Journey

Planning of 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 is 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 replatforming 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 configure and 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 for your data storage (plus any replication costs) until you fail over. This means that you simply pay for what you use and when you use it.

2.3 Design

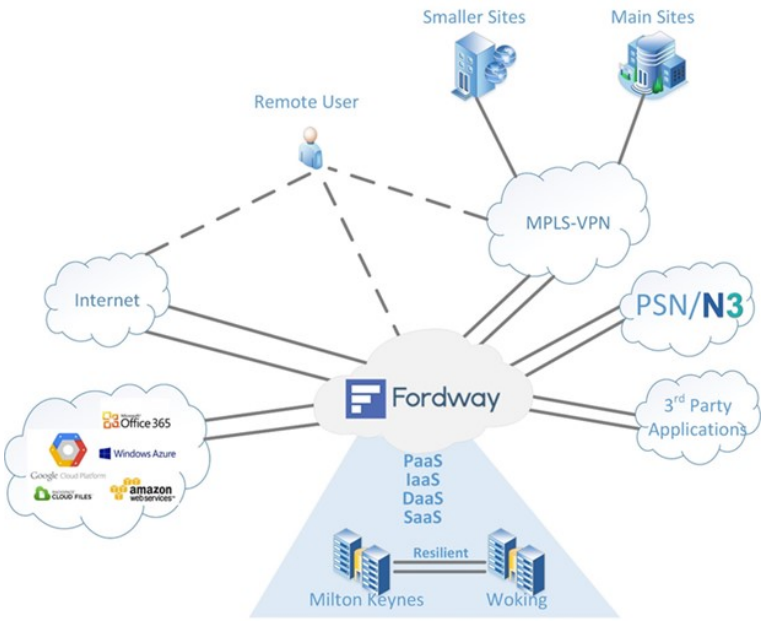
When the analysis has been completed, and a decision about which services can be moved to which type of service, the next step is to size and secure the chosen cloud services, taking into consideration the required agility and elasticity i.e. 'just in time' provisioning, utilisation charging and burst capabilities.

There are a number of areas to review, including:

- **Consolidation opportunities:** enabling costs to be cut by reducing the number of environments to license, secure and manage.
- **Review policies:** do you need a test and development environment available 24 x 7 x 365? Most in-house services run this as they 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, if you could shut down the services that are not needed 60% of the week, you benefit from 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. It will greatly help if these processes are automated. 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.

- **Resilience and availability:** map your services to the required system Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) to meet the organisation's business continuity requirements. Disaster Recovery requirements may be achieved through data replication across multiple domains with a single provider, or for greater resilience, environment replication to a separate cloud provider. SaaS services should be natively resilient and offer a suitable availability SLA; this is an issue to address with the provider as part of the service selection criteria.
- **Design flexibility:** this should enable organisations to adopt different platforms or alternative cloud suppliers, however this is not a simple process, major cloud providers each have different instance families, different storage types and standard configurations. At the moment this is only feasible using third party tools, increasing complexity and cost.



Example of Fordway hybrid cloud service

To manage cloud effectively there have to be clear definitions and ownership of the boundaries of the service levels. IaaS, i.e. a hosted hypervisor plus storage and connectivity, is the base layer of any service. It then needs to host the OS, middleware and service layer (which makes it PaaS if provided by the cloud service), which then run and deliver the application logic and interface (SaaS if delivered by the cloud provider). These definitions address computer power,

operating system, server roles and their associated configurations, middleware such as JBOSS, BizTalk, SQL or Sharepoint, applications and interfaces. They also define, responsibilities for security such as patching, backup and recovery.

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, 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.

It is also important to make sure that cloud providers' interfaces are as standard as possible to ensure service interoperability and ease migration. 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. 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 people aligned and prepared, give them clear guidance and manage the exceptions that will undoubtedly occur.

4. 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, for IT Service Delivery 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 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, and that the providers either allow visibility of their service or 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 Cloud Platform). Services such as Fordway's CMaaS can carry out this monitoring from a single pane of glass and can also be used to monitor traditional in house IT services, plus hosted and private cloud services where agents can be deployed or gateways installed into the monitored environment. Network monitoring is also provided and the results integrate into event correlation and are then displayed on custom HTML5 dashboards which offer policy-based SLA measurement.

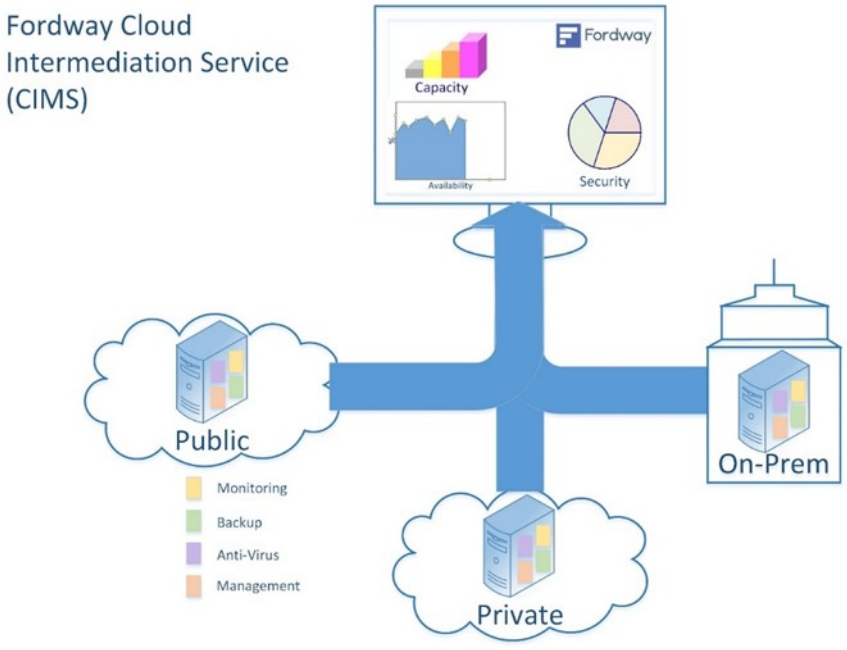
5. Managing Hybrid Cloud

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, with user self-service through web portals. However, most organisations prefer, and in many cases need, a human voice plus organisation specific information from their services. Additionally, there may be several cloud providers who collectively supply your IT service.

Thus we are seeing the introduction of cloud management services which enable 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. Simplistically Cloud Management is 'lightweight' SIAM (Service Integration and Management), with the controls, processes and principles of the discipline but without the hefty price tag and long term contractual commitments 'full' SIAM has historically involved.

Expert advice at any stage

Choosing the right mix of cloud services and the most appropriate provider 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), Identify Management (IDAMS), plus 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 organisations get what they need from their suppliers, and that services are portable and futureproof. 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 host more challenging 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.