Managing Your Cloud Transition

Microsoft Azure for Government

June 2018

Contents

Summary

When faced with the mandate to move to the cloud, what is your agency's response? Do you rush in head-first? Or do you hang back for as long as possible?

Earlier in 2018, the Digital Transformation Agency's (DTA) cloud strategy laid out a vision for transforming government services to become more modern and flexible. However, according to a global study published by McKinsey[1], only 26% of organisations say their transformation has been very or completely successful.

Those odds are daunting for agencies who are contemplating a move to the cloud. These disheartening results happen when the project fails to account for the common sticking points in a transformation – sticking points that often fall outside the narrow realm of a technology upgrade. By addressing these issues before the project begins, organisations can double their success rate and avoid common traps that can halt a digital transformation. In this white paper, we aim to cover what, in our experience, are the critical factors when starting down the road to cloud.

These include:

- Common risks organisations face and how they can be mitigated
- Common misconceptions about the cloud and digital transformation
- How your corporate culture plays into your success in the cloud
- Why governance needs to dovetail with culture
- A starting point for your cloud migration strategy.

Did you know?

Digital transformation is an imperative for government. We've done our own summary of the DTA's digital strategy. Check out our seven principles.

Risks & Challenges

Every organisation is different but, in our experience, there are four key risks and challenges our customers are seeing as they transition to the cloud.

1. Knowledge

The most common rough patch projects can run into is a lack of knowledge. It's unproductive to start planning your cloud migration strategy until everyone involved has a foundation of knowledge to work from. The cloud is a relatively new and ever-evolving area of technology and specialisation. Gaps can exist between what and how much individual agencies know about this technology.

This lack of knowledge can interfere in two ways:

- Between the internal IT team and the supplier: If an organisation's internal team's knowledge is lacking, it can create friction points between the agency and the supplier. The time that could be spent planning is taken up with time spent educating the IT team, which can push deadlines and take up resources.

- Between the internal IT team and the remainder of the business: A lack of knowledge or difficulty communicating this knowledge can also have strategic ramifications for the digital transformation. The scope of the project can be difficult to define if the proper level of knowledge doesn't exist in the business. Government agencies might not realise there are many benefits in moving all applications to the cloud, rather than just one.

To mitigate this risk, it is imperative to identify company education. The questions to ask are:

- Who will be affected by the digital transformation, and what are their information needs? Are there external partners like vendors that need to be updated on the use of cloud and the operating model?
- How much do staff, partners, and vendors already know about the subject?
- What is the best way to teach them? Bring the company up to a basic level of knowledge, educate key people and wait for knowledge to trickle down, or both?

List estimates of how much knowledge all parties already have to see the level of education needed. Then, allocate education time based on the level of importance. The IT department and nominated cloud champions may need an intensive week of education, while the rest of the company might only need a few hours. The answers to these questions and knowledge estimates will create the education strategy. Committing to rapid staff development and training will mean your transition rapidly gains momentum and isn't plagued by technical hurdles.

2. Technical Debt

The other common sticking point in transitioning to the cloud is the appearance and management of technical debt. Technical debt is an inevitability for any agency – it's the discrepancy between the current and desired state and the cost of completely bringing the technology up to date. Time spent not updating technology accrues 'interest' payments: extra effort needed to fix and upgrade systems. Existing technical debt, like out-of-date systems, misplaced data, and scattered records can stop a project in its tracks, as overcoming it is too hard and too costly. Of course, this only accrues more technical debt.

Technical debt is challenging to solve, and the best approach, if the organisation is not experienced in transformation, is to get outside advice. Managing technical debt is highly individual and depends on the level of functionality that the organisation requires. For guidance on how to implement a cloud strategy, Veritec has a discovery service that covers overcoming, addressing, or managing technical debt. For more-experienced organisations:

1. Identify what can be left behind and replaced by other applications.

2. Identify what can be modernised or even rebuilt.

3. Identify technical debt that has the potential to become valuable intellectual property. Is there a possible solution or innovation that can be monetised?

4. Determine a backlog priority for migration. Start the transition with applications that have manageable technical debt and provide immediate value once delivered and managed in a cloud environment. For example, applications that have been suffering from a lack of high availability or perform poorly under high load are top candidates for cloud adoption.

3. Internal Resistance

As with most projects that require changes to processes and procedures, a move to the cloud is likely to be met with some level of internal resistance. Some agencies may have dabbled in previous cloud projects and felt that it didn't work for them; others have successfully migrated but have discovered there is a lack of correctly skilled resources to support it; and others may feel that they're taking on unjustified risks.

The first step to making a clear transformation is to properly allocate senior leadership personnel to the project. Transformation doesn't happen part-time – it needs full-time attention. Senior leadership need to be educated on what the change entails, be committed to the innovation, champion the vision, and help execute the change by coordinating people. Senior champions can also help broker compromises to situations that might otherwise result in impasses within the business. For example, their senior position can mediate between concerns from the CFO about the budget running over, and concerns from the CIO about the solution not being thorough enough.

The second step is creating cloud champions at all levels. A common occurrence is getting senior leadership who have an agenda for radical change, but lower-level employees lack the motivation or understanding to complete that agenda. That motivation for change then fizzles out. Digital transformation therefore needs a combination of top-down and bottom-up approaches to change. A useful way of thinking about organisational change is that it's like the way mobile phone signals transmit over a country – signals are sent to base stations which wirelessly transmit information to mobiles and tablets. Without enough base stations for an area, the signal degrades. The same process happens with company information distribution. There needs to be people at all levels to make sure the change happens. To address this, nominate cloud champions by how close their contact is with key parts of the organisation. Important stakeholders should all spend more time being educated, as they can then educate others.

4. Risks of Delaying

The biggest risk of all is not transitioning to the cloud. There is one overarching risk with delaying the move to the cloud, and that is not delivering the services that citizens expect. In their private lives, citizens interact with businesses when and where they choose. They create digital identities. Businesses use this information to streamline the interaction and tailor the experience. With businesses, the interactions are seamless and instantaneous. With government, interactions can be laborious, full of paper processes, and with service points giving inconsistent advice.

Increasingly, government agencies face competition. We see an emerging market of private-sector providers who fill the gaps left by government. An agency has a convoluted application process, so a provider makes the application on the citizen's behalf – and charges a premium. The risk to government is losing relevance and the opportunity to engage citizens. Technologies enable government to meet those emerging needs by being more responsive. Every agency's cloud migration will be different. The cloud allows you to start small, migrate one piece of infrastructure, and move forward at your own pace. Setting that pace and charting the next steps – that's where an experienced guide can help. It's easier than you think.

Get Your Facts Straight

There's a lot of misinformation and outdated thinking about the cloud. Here's what the landscape looks like today.

There'll always be resistance to change, but even more so if ingrained habits are challenged, including staff's professional attachment to existing infrastructure. You may encounter rusted-on cloud sceptics. If staff or service providers feel pressured to make changes that appear to challenge their status, they may dig their heels in: your cloud teams will face reluctant compliance rather than willing collaboration.

- There is still a lot of fear and misinformation about what the cloud is and how secure it is. In a lot of respects, the cloud is now more secure than a lot of organisations' on-premises services. You may have a locked room in the basement that still contains asbestos because you cannot move the server racks for fear that they won't turn back on again. The cloud can help mitigate these risks and single points of failure, and help you bring your building up to code. Security, compliance, and best-practice concepts are no different to your on-premises infrastructure except that they are in the cloud. There is a perception that, just because you can touch and see your servers in a rack and you're sitting behind a firewall, you are more secure than being in the cloud: think again. Correctly configured, your cloud infrastructure can be just as secure as your on-premises services, if not more so.

- Cloud evangelists will tell you that the cloud is always cheaper. Cloud technology can be cheaper, but the attributes that make it cheaper can also make it more expensive to run. When shipping workloads to the cloud, often you can achieve better prices. But because of the scalable nature of the cloud, the cost will scale with demand. When the solution first begins, due to the infrastructure, the demand can skyrocket, and the usage costs will increase as well. Unless the internal structures have been set up to control for this, the price will be as expensive, or more expensive, than hardware solutions. To remedy this, people need to think about the cloud with the same depth of consideration as physical hardware. It will allow for greater flexibility and innovation, but systems need to be set in place for the management of cost and overruns in demand and computing power.

The most dangerous cultural attitudes towards cloud adoption are the tendency to put up barriers to prevent the changing of ways.

- Cloud installation needs a shift in how software development is planned. A crucial misconception is that all projects evolve the same way. For example, think about development software environments. For a development project under legacy systems, a project might need eight environments for testing, deployment, and running, and they would need those eight environments to run for the whole duration of the software project development. Using a cloud solution, projects are able to switch on and off environments at different stages of the project and can automate this process. While the planning process using 'older systems' thinking will still work, government won't be able to take advantage of the benefits that the cloud brings. Planning in cloud environments requires thinking about not only how to accomplish the project, but how best to use cloud technologies to accomplish it faster or more efficiently.

- The shift to managed infrastructure can mean a feeling of loss of control. Currently, someone else is responsible for patching servers and software and maintaining infrastructure. This invokes a kind of protectiveness, and a fear that when data is in the public cloud it can't be managed. The idea that projects don't need an infrastructure manager is incorrect. However, it is correct that new skills need to be developed in the move to the cloud. The cultural shift that therefore needs to happen is for employees to see the cloud as an opportunity to re-learn, re-skill, and adapt their job skills and qualifications to a new role.

- There will always be some people within a government department who believe that a transition to the cloud is impossible because it's too big, or too small, or has too many legacy applications. The most dangerous cultural attitudes towards cloud adoption are the tendency to put up barriers to prevent the changing of ways. This also manifests in a negativity towards the capacity of the cloud and the ways government can take advantage of it. To tackle the attitude that security and data sovereignty issues are impossible boundaries, demonstrate how their challenges will be overcome. Intelligent planning and detail on the various cloud service configurations can address these problems. A recent example is the CIA, which built its own private cloud[2] to provide efficiency to employees and other agencies while maintaining security. Good planning and thorough investigation can address fear and uncertainty.

- Something we hear frequently from our clients is that they believe adopting the cloud is risky. Cloud services are only as risky as the plans make them. Employing secure data-storage methods can address risks and issues. Reframe the discussion around implementation by listing the risks that the department is exposed to by not moving to the cloud. These may include: losing the opportunity to take advantage of the investment in technology, reliability, and functionality that cloud vendors are making; losing access to machine learning; difficulty making infrastructure available for increased demand or requiring scalability that they can't access; and all the risks associated with physical infrastructure, like failure or updates.

Culture is Key

Don't migrate your mistakes. To succeed in the cloud, you've got to change the way you work. Change your corporate culture to best benefit from the cloud.

Leading a move to the cloud requires more than technical transformation. It requires a shift in hardware, software, and processes, but most importantly a shift in culture. The cloud mindset affects changes in planning projects, cost structures, project execution, and educating and developing staff. There are some essentials that cloud transformation is built off, and some common cultural misconceptions that, unless addressed, will undercut the benefit of the transformation and may even sabotage it.

Cloud gets built on a stable cultural base. The cultural shift to the cloud requires as much strategic thinking as planning the technical aspects of the migration. The company needs to plan and account for the cultural change that will need to occur with the cloud. This happens in a series of steps:

1. Assess the department culture for common misconceptions, above. Then, strategise about how to combat those misconceptions.

2. Assess what levels of expertise exist in your staff. Staff might be your most capable asset, or there may be a skill gap that exists. To find those gaps, consider a series of workshops and assessments to locate and define them. From there, an education campaign is required to address the cultural changes that will occur

3. Assess the requirements for ongoing maintenance. An agency needs to determine its capacity to manage its environments after moving to the cloud. How will the solution be maintained after installation? Who'll be responsible for it? Do they have the necessary experience? Creating this experience base will make sure that the project doesn't falter after it's been installed.

4. It's also important to note that an agency is unlikely to move entirely to the cloud. There are some applications and solutions that are best suited to an on-premises environment. The key is to define the amount of cloud necessary, then build the capability for that.

5. The most important way to organise cultural change is to demonstrate that cloud technology works using a successful project. If it's not executed well, people will revert to the old ways of doing things. Therefore, it's essential to get the first project right. By addressing these common misconceptions and creating the right culture, you build the solid bedrock to support your technological transformation.

There are real benefits to automation, infrastructure as code, DevOps and Continuous Delivery, and they're all enabled or enhanced within the cloud. However, they also all require a cultural shift before they can be implemented.

Get Your Governance into Gear

Without strong governance you cannot transform your business.

Before you start moving to the cloud, you need to have the right amount of governance in place to both benefit from the cloud and mitigate risks. Governance takes many forms, but we will be focusing on three areas: building governance into the cloud, governing identity within the cloud, and cloud economics.

Built-in Governance

When your cloud technologies are implemented with governance in mind, you can take advantage of a hyper-scale cloud without exposing yourself to the risks associated with having nearly unlimited computing within arms' reach (for a price).

Managing your enterprise architecture and billing:

Billing within the cloud is a primary concern for any organisation. Thankfully, there are many service providers that provide detailed spending projections and reporting. Your hyper-scale cloud provider (Azure) will provide you with monitoring alerting for spending as well as soft and hard spending limits.

Cloud scaffold:

It's imperative to design your cloud environment and scaffold it based on your organisation's unique needs before you start loading resources into it. Just like when building a house, you wouldn't build the foundation last.

Subscription setup and management:

Putting thought into how your cloud subscriptions are organised ties into the section below on cloud economics. Being able to control spending by division or branch within the company, and logically separating out production and non-production environments, gives you the granular control over your finances necessary to move forward.

Identity management:

This is also covered in greater detail below. Ensuring your organisational identities are managed correctly before moving to the cloud will enable your governance and security to succeed within the cloud.

Security and compliance:

Cloud providers offer native tools to enhance security and compliance. Azure's Log Analytics platform gives security staff within the organisation a bird's-eye view of both cloud services and on-premises equipment. However, it's imperative to determine your auditing needs beforehand, working through guidance documents like the Information Security Manual and working with technical staff to implement controls and logging.

Workload management:

Working with a hyper-scale cloud provider allows you to take advantage of on-demand computing for your workloads. Unfortunately, this can quickly spiral out of control. Planning out each of your workloads and reviewing the Service Level Agreements will allow you to determine the level of availability you need to aim for. Allowing your applications to automatically scale up to keep pace with demand is convenient but must be tempered with an eye on the what your organisation is comfortable spending.

Automation:

Using the automation tools built into the cloud, it's now possible to manage your cloud resources in ways that were not previously possible – for example, shutting down computing resources when they're not required. It's a different way of doing business when you're being billed by the minute, and it can save your organisation money by designing around this and considering which resources aren't necessary outside of your core hours.

Identity Management

How do you currently manage access rights? We see many organisations with ad hoc identity management. Staff members have multiple profiles scattered across systems. And when they leave the organisation, their accounts are left active, raising risks of a breach. Some agencies underestimate the complexity of solving identity management. This is more than just managing basic authentication and whether a user can log on to their device. It's a matter of managing individuals' ICT identity across the enterprise. How do rights and privileges travel with the individual? And how will your agency detach those rights and privileges when the individual leaves? If a user's identity isn't being managed correctly on-premises, moving to the cloud will only compound that problem further.

Cloud Economics

Cloud economics is the principles, costs and benefits of cloud computing. This involves procurement, billing and resource management through to demonstrating a return on investment. Analysing these factors will help you to determine your next cloud step. It's important to ensure your finance teams are across these changes. Moving to the cloud will involve a fundamental shift in how IT is budgeted. Instead of an initial capital expenditure on hardware and software licencing, followed by trailing maintenance agreements which must be renewed, in the cloud your spending is primarily operational expenditure, with ongoing billing based on exactly what you use. This makes it more transparent and easier to manage.

Plan Your Way to Success

How to plan your migration.

Start Small

How do you eat an elephant? One bite at a time. It's an old saying, but it still applies. A successful cloud migration is built from tackling tasks one at a time. In order to decide what to do first, you need to define what success looks like. This is where your cloud strategy comes into play. Your cloud strategy can be broad and non-specific: move all business applications into the cloud, for example (don't overcook it). Decide the scale of the change you want to make. Once the company has been educated on the scope of the project, they can decide how large the level of change will be. There are several philosophies on how to adjust the size of changes. Organisations can choose to start small by moving a non-business-critical application to the cloud. This allows teams to test processes, spot potential issues, and learn how to implement cloud solutions. The approach also reveals areas where things might go wrong on a larger scale, minimising critical errors. However, projects that are too small in scale don't spot the problems with larger application changes.

Once this is defined, break down all the steps that need to be taken to get there. Then assess the risk associated with each application, service or workload and migrate them accordingly. Some business applications are more suitable to move to the cloud than others. At Veritec, we see some organisations transitioning their business-critical applications in the first phase of their venture to the cloud. This isn't always the best approach. As Booz and Co[3] have noted, and as we've discussed in previous blog posts, it's better to start small. Move commodity-based applications such as email and websites, analyse the success of that migration in terms of business objectives and use that information to plan the business case for the next phase. Easy candidates for migration can be applications like desktop productivity or applications that are already a Software as a Service, like a CRM (low risk). Once smaller applications are moved, start planning the bigger, more complex, and riskier applications that can be broken into logical components.

> **Move commodity-based applications such as email and websites, analyse the success of that migration in terms of business objectives and use that information to plan the business case for the next phase.**

Don’t be afraid of hybrid cloud. If you have a legacy application that everybody is afraid to touch running on a mainframe, for example, move the application tier to the cloud and leave the data on-premises. Remember your virtualisation journey: the lessons you learned then are just as applicable today in the cloud. Also, don’t be afraid to make mistakes. The true value of the cloud is the ability to innovate fast. If something doesn’t work the first time, tear it down and try again.

A service map is a good tool to assist in planning. After the planning work is done, map the business service offering as it currently looks. Use this layout to identify which parts need to be moved into the cloud, and in which order. You can also use this to decide which aspects are suitable to merge together, and which can be discarded. Then, once you have a list of applications, you can build a risk profile under each application to decide what should be prioritised first.

Define Your Cloud Architecture

Once the strategy and plan have been laid out, map the architecture of how the organisation will look in the cloud. Questions that this map should answer are:

- How will organisational compliance and governance requirements be met?
- What will the services look like in the cloud? How will they talk to each other? How will they be managed?
- How will resource groups be set up?
- How will identities be managed?
- How will customers (internal and external) connect?
- What monitoring services are required?
- How will security be maintained?
- How do we scale (horizontally and vertically)?
- How are critical business services maintained (reserved instances)?
- What will your Business Continuity Plan look like during and after migration?
    - Backup
    - High Availability
    - Disaster Recovery

Automate

The automation mindset needs to permeate the project, from planning to direction and finally to execution. Always ask: "Can what we just did be repeated, reused, and recycled?" Examples of automating processes that save time are the initiation of a virtual machine and scaling up of capacity using scale sets. The faster the agency can transition to infrastructure as code, the better the migration will be.

Seek Advice

Advice is essential: if the agency is unsure or hasn't conducted a cloud migration before, they can benefit from an expert opinion on their cloud maturity or migration. It's a good idea to get advice from a fresh set of eyes up front, especially on cloud architecture, governance and compliance. If you want to start your migration with the best possible chance of success, setting up your tenancy with this in mind will give you the best possible result and reduce the risk of failure. There are a couple of events that identify when advice is needed during the migration – if, in the execution of your plan, a migration hits a roadblock or fails, seek advice and try again, or move on to the next candidate, but keep moving forward. Another useful event is a retrospective evaluation. When evaluating the success or failure of a particular migration, it's a good idea to look back and evaluate with an expert eye what went well, what went wrong, and where things could have been improved. Creating a continuous feedback loop will make each migration more efficient and successful.

Applying These Principles

Rinse and repeat, and you're on your way to your digital transformation. The advantage to this approach is that every application, component or workload moved builds momentum and confidence for the organisation. The benefits in time, cost, and functionality will become apparent and the limitations of legacy applications will become obvious. Also, this step-by-step approach de-risks larger app transitions, as risks are identified early while working on less-critical areas of your business. Remember, Rome wasn't built in a day and, just like Rome, your digital transformation will not happen overnight – it is a journey, but an easier one to start than you think.

veritec
[SOLVED]

Contact us

Contact us today to start your digital transformation journey.

p: 02 6154 5900
e: info@veritec.com.au
w: veritec.com.au

References

1. David Jacquemont, Dana Maor, Angelika Reich, McKinsey&Company, ‘How to beat the transformation odds’, survey 2015, accessed 5 April 2018, https://www.mckinsey.com/business-functions/organization/our-insights/how-to-beat-the-transformation-odds

2. ‘CIA Creates a Cloud: An Interview with CIA’s Chief Information Officer’, Doug Wolfe on Cloud Computing at the Agency, accessed 4 April 2018, https://www.cia.gov/news-information/featured-story-archive/2014-featured-story-archive/cia-creates-a-cloud.html

3. Booz and Co, PWC, ‘The Cloud Is Ready for You Are You Ready For the Cloud’, accessed 10 April 2018, https://www.strategyand.pwc.com/media/file/Cloud_Is_Ready_for_You.pdf

veritec
[SOLVED]

Azure