

Journey to the Cloud

A Guide to Overcome Common Cloud Concerns

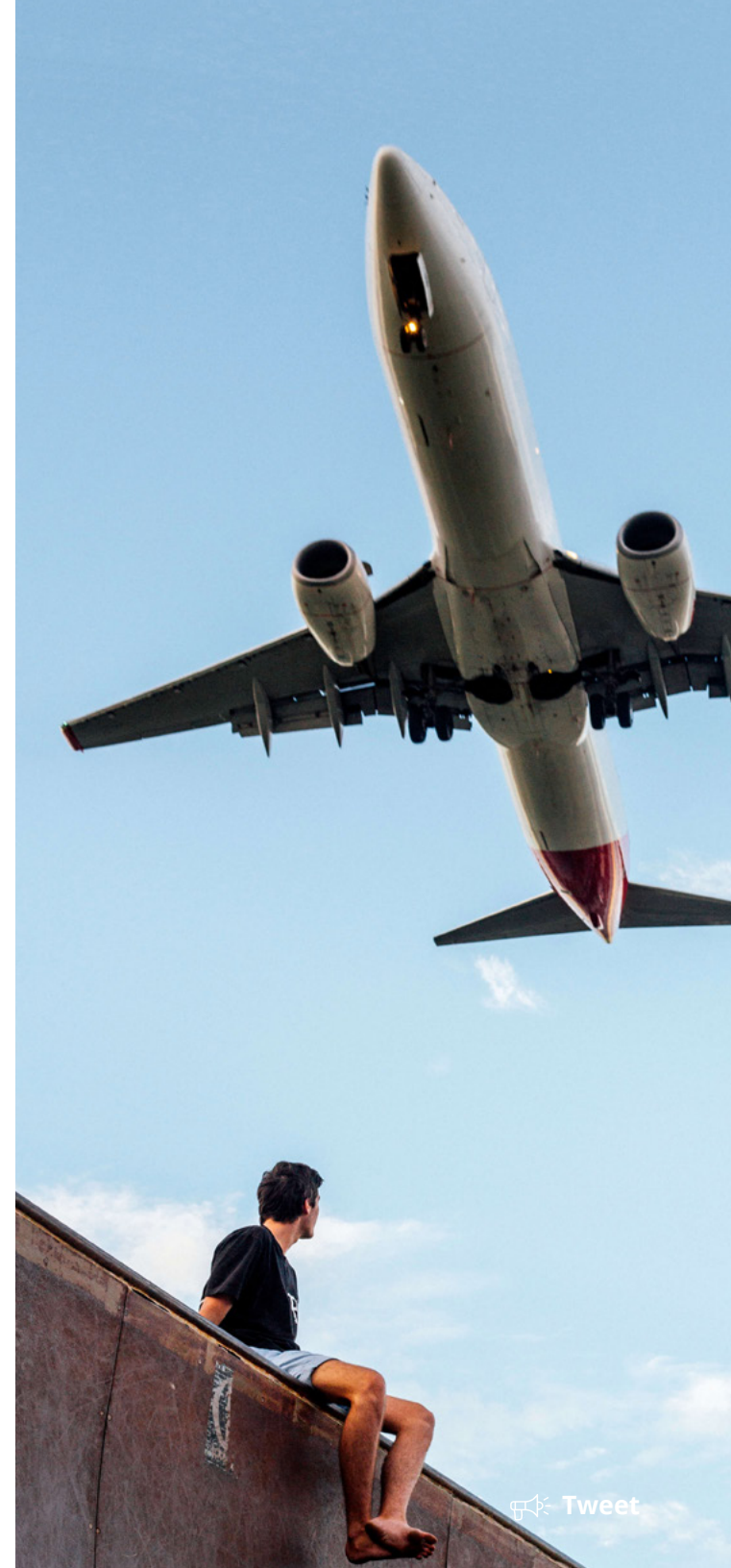


((CENTRIC))

CentricConsulting.com

Table of Contents

Cloud Control: Who's piloting this journey?	5
Cloud Security: Is your cloud data safe?	9
Cloud Costs: What are the savings and benefits?	14
Cloud Transition: How do you get people onboard with change?	19
Cloud Readiness Checklist	26



Guide Summary

When transitioning to the cloud, it can be hard to get off the ground. Like an airplane taking off, it takes people, power, and skill to soar safely and successfully.

For businesses looking to improve their IT functions and processes, the cloud is the place to be. In fact, as more companies move off-prem to reduce costs, increase security, expand their global reach and accelerate innovation, cloud spending is growing nearly 20 percent a year, totaling more than \$160 billion worldwide. More and more IT workloads will soon be processed in the cloud than on-premise, which is causing major change in IT.

But for any business, cloud transformations are full throttle implementations. The rate of acceleration and magnitude of change present complex technical and organizational challenges. If you're thinking of making a journey to the cloud, there are several things to carefully consider before take off to safely reach your destination: control, security, cost, and change management.

In our guide, we share strategies to overcome these common cloud concerns, making your transition smoother and more effective.

Chapter 1 - Cloud Control: Who's piloting this journey? By Kevin Bracy

One of the biggest ongoing challenges to any change is control. As humans, we want to know that we're in charge and navigating our own success. When considering cloud computing, we hear about the benefits: flexibility, scalability, reliability, global access. But we still have a sense that we are losing control of our systems when we turn them over to a cloud provider. Kevin assuages those concerns, and shares how moving to the cloud can even give you more control over your IT assets.

Chapter 2 - Cloud Security: Is your cloud data safe? By Paul Holway

Moving to the cloud comes with risks, which is why a review of safety measures and protocol is critical before every take off. Any mention of migration to the cloud brings up this question: Is it secure? Whether migrating to a SaaS platform for systems - such as CRM, email, document storage - or upgrading your infrastructure and developer capabilities, organizations of all sizes, across startups to regulated industries, are asking this question. While there is no one-size-fits-all answer to the question, Paul outlines a set of principles to follow.

Chapter 3 - Cloud Costs: What are the savings and benefits? By Dion Dunn

How do you know you're getting a good deal on your journey? Not all infrastructure costs are created equal nor are the savings. Cloud cost savings tend to be realized in different ways and at different times than the normal IT spend cycle of the past. Dion dives into the details of cloud cost structure, including resources for you to estimate your spend.

Chapter 4 - Cloud Transition: How do you get people onboard with change? By Gina Heffner

It takes a cohesive crew to successfully journey to the cloud. However, many businesses in the midst of a cloud transition may worry about the state of their IT crew, wondering how their roles will fit into the new public cloud service. Fortunately, the cloud is not replacing IT staff, it is simply changing what IT staff do. But this is causing enterprises to pause and assess "how effectively are we managing the people change?" Gina outlines steps to get your people onboard.



Chapter 1

Cloud Control: Who's piloting this journey?



One of the biggest ongoing challenges that comes with change is “control.” As humans, we want to know that we’re in charge and are able to control and navigate our success.

When looking at cloud computing, we hear about the benefits: flexibility, scalability, reliability, global access. But we still have a sense that we are losing control of our systems when we turn them over to cloud provider. Are we the pilots of this journey, or is the cloud provider?

There are several ways that we feel the loss of direct control:

- We don’t own the assets.
- We can’t physically touch the hardware where the code or data resides.
- When something goes wrong, we can’t “brute force” our way to a solution by throwing a small army of IT professionals at the problem.

Why then, should you move forward with a cloud solution? The benefits are just that good.

How to Stay in Control

Let's look at three typical fears of losing control and how to mitigate them:

1 - ASSET OWNERSHIP

A common aspect: outsourcing the ownership and maintenance of assets that are not the core focus of your business.

Very few companies want their capital tied up in real estate, buildings, or other capital intensive resources. Similarly, enabling your business to outsource computing and network power to the cloud is a great opportunity for the business to free capital for other purposes, while ensuring applications keep running round-the-clock.

Services (backups, failover, recovery, redundancy) are limited by the hardware that is purchased. By "renting" computing power from the cloud, your monthly payment will buy a higher level of service than what you can buy through ownership.

Cloud tools also give you the ability to configure point-in-time scaling and failover solutions, helping mitigate risks and quickly address issues that may come up in the environment.

2 - SECURITY

Who has better security: The local credit union with assets of \$15 million, or Bank of America with assets over \$1 trillion? The same analogy holds in the cloud.

Cloud providers have the scale to be able to provide a large team of security experts that are constantly working to secure the cloud system. This is also an area where customer and vendor interests are closely aligned. Physical security in cloud hosting data centers will nearly always exceed the level of security obtainable by hosting your environment on-premise.

If there is a security breach on a cloud system, it's certainly an issue for the individual client. It will also have a huge impact on the revenue of the cloud provider as other customers will move their systems to ensure they are not impacted by a breach. Hence, it's in the best interest of the cloud provider to focus on robust security measures. Additionally, security is based on the architecture and management of your cloud environment. You can deploy systems that adhere to the security level that fits your business.

Finally, the classic outsourcing argument is relevant to the cloud discussion. Cloud computing is the focus of cloud providers. Hence, providers dedicate people, time, and budget to ensuring that they have a very well secured system in place.

Security is not a cost center line item that has to be grudgingly paid for by the business. It is the business and gets focus as part of securing top line revenue.

3 - VENDOR PERFORMANCE

If I move my systems to a cloud vendor, will I be at the mercy of a big cloud company that will run up prices or provide poor service? Will I need to commit to a long-term contract to get pricing that is competitive with what I could provide in my own data center?

Vendor performance is always a concern. Fortunately, with cloud services, a number of competitive components are embedded into the system to mitigate these risks and concerns:

Contracts – Many plans are short term (12 months or less) or pay-as-you-go. Cloud computing power is provided on a

commodity basis and is widely available from a variety of providers, so long-term contracts are not common.

Tooling - A new suite of software tools has been created that enables multi-cloud solutions, so you can use multiple vendors or migrate to a different cloud provider should your current partner not work out. Cloud services are created in a standardized fashion, which allows for portability. No more “UNIX” versus “Windows” debates that lock you into a particular platform. This gives you much more flexibility than if your systems were situated with a hosting provider or a shared data center.



Final Thoughts on Cloud Control

Similar to any other change in technology, cloud requires a change in perspective and approach. Making those changes can be difficult as they will drive changes to the IT organization, the relationship between IT and the business, and how IT services are provided. This means people, processes, and technology will all need to transform and that is difficult.

Concerns about control in the cloud can all be addressed and should not be a reason to hold you back from exploring the benefits that the cloud has to offer. The data and applications are still yours and you will continue to be in charge of how they are used. It is time to trust that you can get your business to the cloud safely.



Chapter 2

Cloud Security:

Is your cloud data safe?



Any mention of cloud migration almost instinctively brings up this question: Is it secure?

All organizations are asking this question - whether upgrading infrastructure and developer capabilities or migrating to a Software as a Service platform for systems like CRM, email, portfolio management, and document storage.

Like flying, your journey to the cloud comes with its own risks and challenges, and ways to keep your data safe.

How to Keep Your Data Safe

We have outlined five of principles to follow to help you secure your cloud footprint:

1 - FIND WHERE YOU'RE ALREADY A CLOUD CONSUMER

You may understand your application portfolio as conscious choices you made as an enterprise. However, Shadow IT - systems and solutions that haven't been approved by the organization - have become more prevalent as departments find workarounds to what they deem as governance

processes slowing innovation down.

Start the journey by understanding what data you may already have in the cloud such as:

- A line of business trying to solve a need by using a cloud-enabled SaaS tool - like Atlassian for project management, GitHub for source control, or Dropbox for saved files.
- Programs operating in your environment to automate a manual process (sometimes outside of IT governance) that may be scraping data and consolidating it into a non-governed data store.
- Internet of Things devices such as printers, cameras, or even light switches that may be connecting to your network and uploading data about usage metrics.

To secure your data, create a catalog of your cloud-based tools and services:

- Conduct a survey of your enterprise-controlled cloud solutions.
- Create a departmental survey of digital tools used for work purposes.

- Perform reconnaissance on your network for applications reaching out to the internet and for frequent user visits to websites that correspond to cloud services. For example, look for log entries that show frequent visits to dropbox.com.

2 - DETERMINE YOUR DATA CLASSIFICATION AND RISK

After understanding your true cloud portfolio, determine your data classification and risk, using common security definitions:

- **Regulated or restricted data** such as Patient Health Information (PHI), payment card information, or non-public financial disclosures
- **Protected data** such as customer and donor lists, employee data
- **Company confidential data** such as internal communications and collaboration

These common data classifications are important, but with the rise of big data and predictive analytics, the ability for other enterprises to find a needle in a haystack has increased. Consider adding an additional attribute to your data:

- **Operational Security (OPSEC):** For example, data that reveals information about your sales and delivery pipeline or potential investments and acquisition targets. Social media posts and photos posted online may contain geographic location information that inadvertently leaks this strategic data, making them an attractive target. Notes on expense reports may also inadvertently leak this strategic data. If this data is critical to your strategy, it should be identified as such.

Create a concise matrix by data classification for each cloud vendor that includes standards to follow on encryption, password security, access control, and separation of duties. For example, one of our healthcare clients achieved HITECH compliance in the cloud by implementing a subset of NIST classifications per data classification and working with cloud providers to certify their solution.

3 - IMPLEMENT MONITORING TOOLS AND TECHNIQUES

Cloud providers offer excellent tools for logging and monitoring your solution, typically far more advanced than can be maintained in an on-premise environment.

For example, the ability to maintain and search Outlook logs in Office 365 would be very costly and difficult to reproduce on an on-premise environment. But in Azure this is a core feature.

It is important your team understands a distinct process of how often and how to appropriately use these tools. For Azure users, read Tad Yoke's recent blog series on securing Azure, including how to use [Office 365 for Legal and Discovery](#).

Even if a vendor does not have adequate security, additional monitoring and detection tools are available. This has allowed some of our mid-size clients to compete and protect their data at a fraction of traditional on-premise costs.

Typically, the tools follow a couple of key categorizations:

- Active monitoring of network threats
- Passive or historical monitoring
- Password compliance and ethical hacking
- Encryption

4 - DEFINE A PROCESS FOR ACCESS AND IDENTITY MANAGEMENT

Identity management is an often overlooked topic when moving to the cloud. On a technical level, solutions such as [Microsoft's Azure Active Directory can help](#).

Just as important is defining a process about how to provision, deprovision, and monitor access to your portfolio. For example, an organization we work with was surprised to see that an SaaS product used to track resumes of candidates contained salary information after hires were made. Because access to resumes was granted by a business user to all hiring managers, they were unaware they were inadvertently revealing salary information for some of their recently hired peers. Defining this process is such an important step in your journey that we've even built dedicated teams for larger clients that focus on monitoring access control and building increased automation strategies to provision, deprovision, and review access levels.

5 - DEVELOP AND COMMUNICATE A CLEAR ACCEPTABLE USE POLICY

Most security breaches typically originate from people not following established policies and standards. Research

shows that a majority of breaches occur from hacking. And, the majority of those hacks result from internal user actions - a combination of phishing or insider action.

As IT plays a decreasing role as the gatekeeper of all technology and increasingly serves more of an overall governance and risk function, organizations require clearer communication to the entire team on the impacts of their actions. Ensure you have a clearly stated policy that covers:

- Appropriate storage, transmission, and destruction of data based on your data classification scheme, broken down by type (i.e. financials, strategic projects, customer lists)
- Password strength and/or use of multi-factor authentication
- Responsibility on the provisioning, deprovisioning, and periodic review of access rights

Ultimately, part of your company on-boarding and regular training has to include security awareness coaching to help your users understand the kind of data they will have access to based on their job role or function and how to effectively handle that data.

Final Thoughts on Cloud Security

While there is no one-size-fits all answer to the question, one thing is clear: More than technology, your journey to the cloud requires you to increase your maturity at vendor management.

The architecture of your IT systems is very important to security - and your freedom to build a system with as little or as much security in the cloud as your on-premise systems. However, the cloud offers more and better tools for the implementation and design of your security solution.

Like disaster recovery, capacity planning, and budgeting, the cloud should cause a mindset and process shift in how you think of security and manage your risk.



Chapter 3

Cloud Costs: What are the savings and benefits?



Cost is a common concern we hear from organizations that are considering a move to the cloud.

Leaders want to know whether it will be more cost effective than the historical way of operating a technology environment - procuring servers, imaging machines, pulling cables, monitoring systems, putting out fires, interfacing applications, backing up data, writing reports, and housing data stores.

Just like with flying, it is all about researching costs, finding the best deal and seeing the value in the journey. Many companies in today's technology environment have found cloud computing more affordable than on-premise services, but also much more advantageous in terms of cost and competitive advantage.

How to Identify Costs and Savings

In this section, we breakdown the costs - including the savings, needs and advantages - of moving to the cloud so you know what to expect.

1 - CLOUD SAVINGS

Not all costs are created equal. Nor are the savings. The cost savings tend to be realized in different ways and at different times than the normal IT spend cycle of the past.

Key differences include:

- **Inception costs** - Spinning up an environment in the cloud will have far less cost than setting up an on-prem environment, however the bill that you get later on after using this new environment may surprise you. For example, companies that are used to doing data replication to feed enterprise reporting may be surprised to see large charges for bandwidth used by APIs for those services. Or, teams may underestimate how growth will be charged. Look at policy closely, because like software licensing, each cloud provider will vary in terms of pricing for both short and long term usage.
- **Intangible cost** - These costs are the benefits of cloud computing such as faster speed to market (benefit), consulting expense (potential cost), and inflexibility of applications or environments (people change cost).

Given the assumption that the cloud will help your organization realize cost savings, what areas should you consider as prime targets for cost reduction? What is the traditional Total Cost of Ownership (TCO) savings associated with going to the cloud? What categories can you take to your CFO to convince them that going to the cloud is a worthwhile investment?

Consider the following list of what it takes to keep an on-prem environment running and put a rough number to these cost buckets:

- **Server Costs** - Hardware: Server, Rack, Infrastructure, PDUs, ToR Switches; Software: OS, Virtualization Licenses
- **Storage Costs** - Storage Disks, HBAs, SAN/FC Switches
- **Network Costs** - Network Hardware – Core/Aggregation Switches, Bandwidth
- **IT Labor Costs** - Server Admin, Virtualization Admin
- **Facilities Costs** - Space, Power, Cooling, Security

Now, take this list of costs and compare it to what it costs to spin up a similar cloud environment - whether through an SaaS vendor, Amazon, Google, or Microsoft. That data should be convincing enough.

2 - CLOUD COSTS

But wait, nothing is free in this world right? There are also costs associated with a cloud environment that you should consider too. Let's look at what those costs are below.

- You will need a subscription fee to pay for this new service.
- Then there are the associated costs with migrating existing environments off on-prem to the cloud. Sometimes applications can follow a "lift and shift" model, making it fairly straightforward in terms of cost. Other times, an existing application may need to be re-engineered to properly exist in a cloud environment as well as take advantage of the cost-related benefits of living in the cloud.
- And let's not forget the operational costs of going to the cloud. In today's competitive environment, where the major cloud providers are offering complex pricing models and subscription approaches, it's become key to have someone internally focused on making sure your usage is optimal and your organization is taking advantage of the cloud vendor's services.

Cloud companies such as Google, Amazon AWS and

Microsoft Azure bundle all those costs together. Taking advantage of their economies of scale yields attractive pricing for customers. Price wars have been becoming increasingly complex over the past few years as these big players start to drive down costs of services.

3 - CLOUD NEEDS

Just migrating to the cloud is a big cost savings, but knowing when and how to use the cloud is where the real savings occur, and each of the cloud service offerings will have a different take on how to avoid cost escalation in their environments.

Think of it a little like the new smart home capabilities. If you have an app on your mobile phone that lets you know that the lights are on in four of the bedrooms, yet you also know that nobody is currently at your house, wouldn't you turn the lights off if you could?

By having someone from your organization watch cloud usage and monitor it for optimal cost savings, you realize a similar benefit. Detailed monitoring techniques and tools that watch resource usage, complex pricing options, flexible peak models, and reservations are beginning to emerge to help with this process.

But it's still wise to invest in the resources you need to manage your cloud environment. Taking your eye off the ball could erase days, weeks or even months' worth of cost savings.

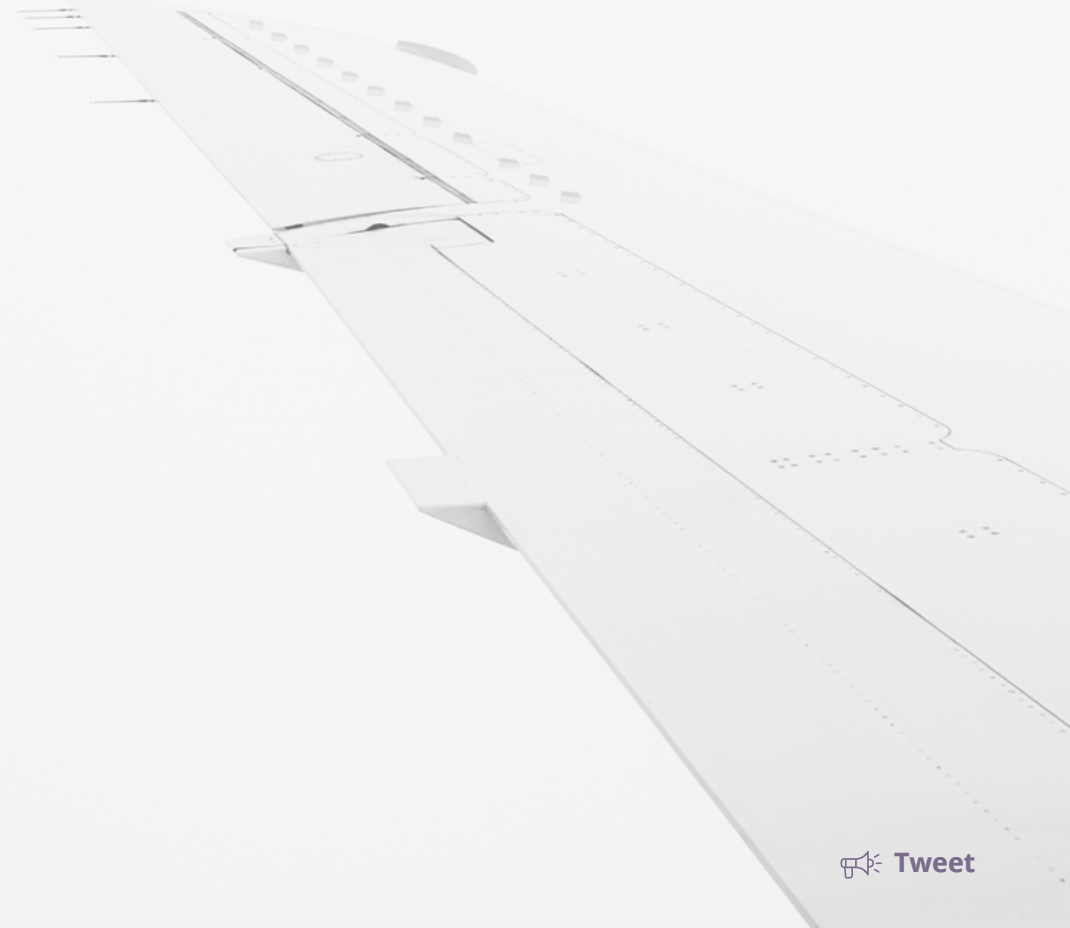
4 - CLOUD ADVANTAGES

But let's get back to the cost advantages of moving to the cloud. One of the biggest advantages of moving to cloud services is the notion that you will 'pay as you go', or only pay for what you are using (as long as you are monitoring it – see above). You can automate systems so they shut down when unused.

Also, there is no need to overbuild environments as typically happens on-premise because you can respond to traffic spikes with dynamic resource allocation.

You will replace large upfront capital costs with low variable costs and pay only for what you use. Although, often times, the vendor's price structure will come down to the volume usage principle - where an increase in people using a tool equals the fees charged. That differs with the cost of entry, which was probably significantly lower.

Other cloud advantages, which can result in cost savings, include the notion of reserving capacity. For some cloud products, you can pay a reduced rate for on-demand services or non-peak times.



Final Thoughts on Cloud Costs

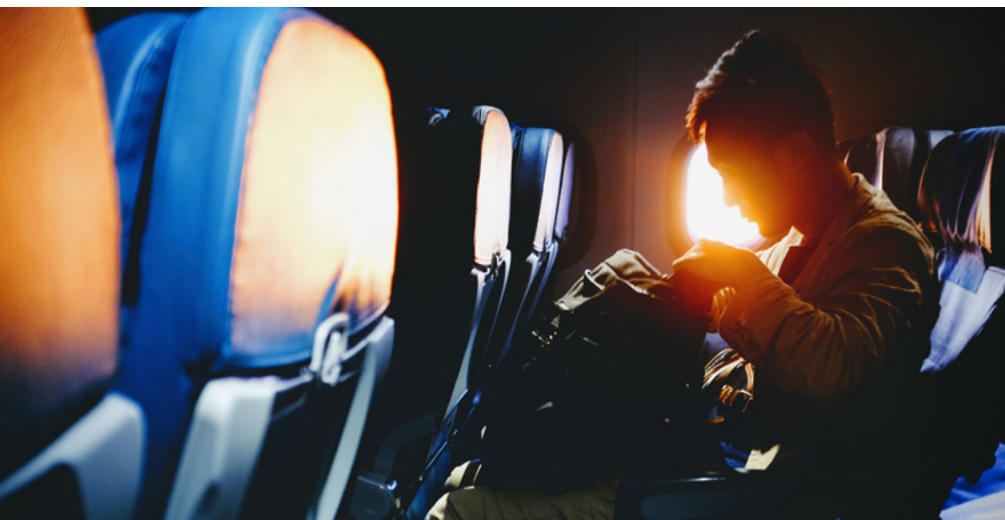
Are you looking to get started on your journey, but want to research how costs would apply to your environment? Explore [Amazon AWS](#) or [Microsoft Azure's](#) TCO calculators.



Chapter 4

Cloud Transition:

How do you get people onboard with change?



Many businesses in the midst of a cloud transition may worry about the state of their IT crew, wondering how their roles will fit into the new public cloud service. Fortunately, the cloud is not replacing IT staff, it is simply changing what IT staff do.

But this is causing enterprises to pause and assess how effectively they're managing the people-side of change so employees are ready and accepting of the shift.

Transitioning to the cloud is no longer an 'if.' It's a when, how fast, and by how much. Taking off on this journey can be bumpy, with the most common cloud challenges being organizational, not IT. Beyond security, top challenges include cloud skills, costs management, compliance, governance and cloud services management, as rated in a 2018 [RightScale Report](#).

For enterprises looking to avoid the turbulence that comes with a cloud transition, building organizational capabilities and better managing and optimizing cloud expertise are top priorities. Enterprises are realizing the speed at which shifting large workload volumes to the cloud requires a cloud-tailored approach to managing organizational change.

So how do enterprises move to the cloud successfully, without sacrificing the integrity of their IT crew? The key is redefining your IT organization's design to ensure a smooth and safe flight.

BUSINESS & IT LEADERSHIP ALIGNMENT

IT Organization Design for Cloud Operations



Org Structure

Alignment to Cloud Services & Delivery Model, IT & Business roles, cross function collaboration, resource levels and skill mix.



Accountabilities

Cloud roles and responsibilities, decision rights, performance goals and SLAs



Cloud Capabilities

People, processes and technology requirements supported by organization structure and resources.



Culture

Moving from Traditional IT to Cloud Based Delivery Model



Governance

Resolving issues of Cloud strategy and Cloud resource allocation, performance management and other cross team matters

ENGAGEMENT

CLOUD SKILLS TRAINING

COMMUNICATIONS

How To Get Your People Onboard With Change

Follow these steps to get your cloud transition process smoothly off the ground:

1 - CREATE A PATH

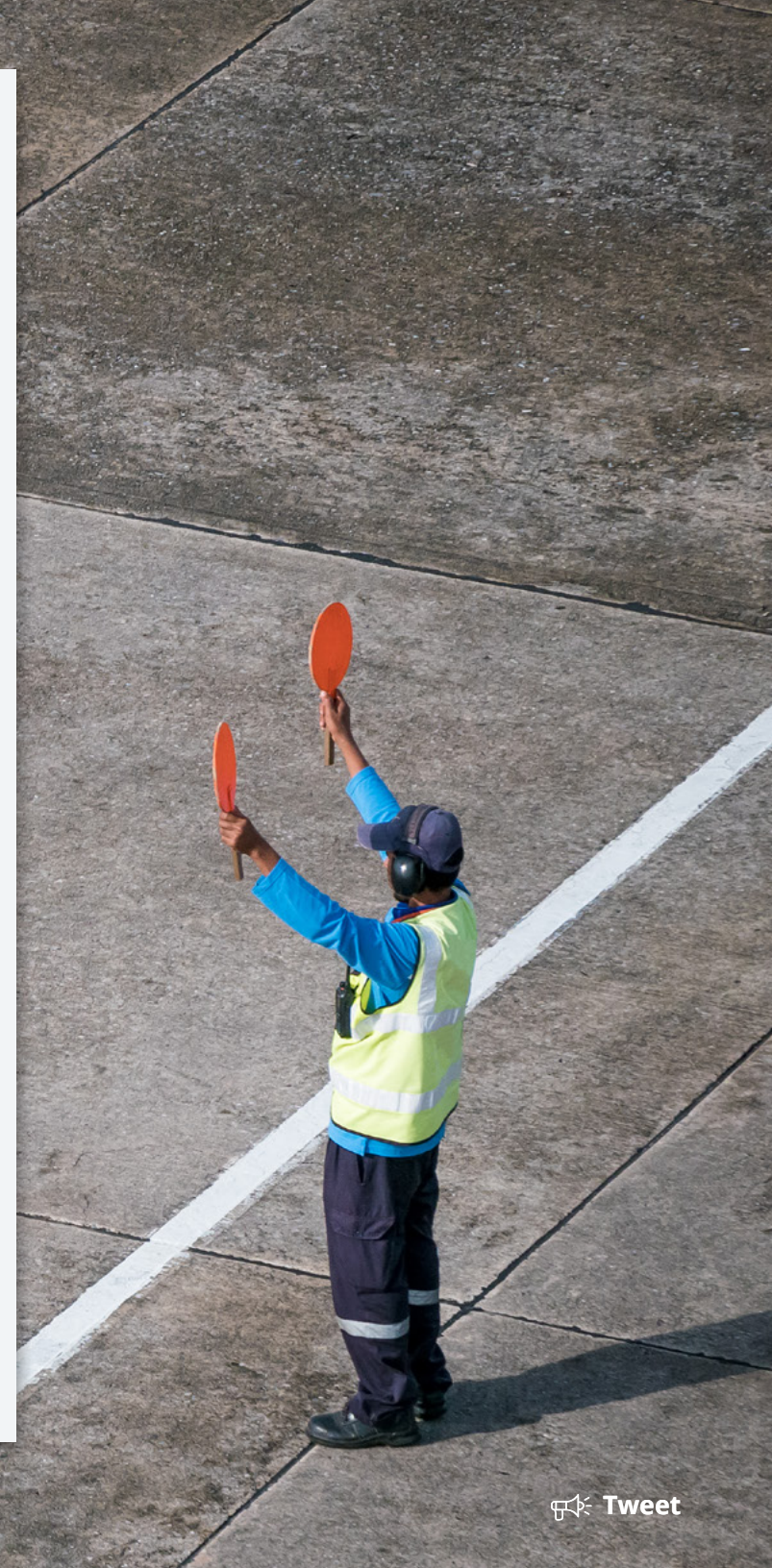
The starting point of any change management project is alignment between business and IT.

Managing change during a cloud transformation initiative begins with everyone being on the same page – knowing the strategy, where we are today, where we are going, and the route we will take to get there. Communication among teams is vital to ensure that everyone involved is on board, and to avoid the extra baggage that often comes along with change.

2 - DEFINE ROLES, AND CREATE NEW ONES

On a flight, every crew member takes part. The pilots fly the plane toward its destination, air traffic control help the pilots navigate, and the flight attendants keep the passengers safe and up to date. The same can be said for a cloud transition project, where each team member plays an important role.

Cloud brings new roles and responsibilities, and a need for organizational structure changes. On-premise roles tend to be hands-on and highly technical, whereas public cloud roles are focused more in management training and orchestration and control.



As you make organizational structure changes, the first thing you'll have to consider is governance, which is key for effective strategy execution and change management. Governance includes: cloud strategy, risk management, and cloud management and operations practices.

- **Cloud Strategy** - Cloud strategic decisions, resource prioritization, technology standards
- **Risk Management** - Information security, data management, regulatory & compliance, accounting, business continuity, vendor management, legal
- **Cloud Management Operations** - Cloud Architecture, Cloud Services Management, Operations Management

The next step is process capability:

- Defining processes with clear accountability for decision making, and communicating how decisions are made and by whom. People, processes, and technology must all be defined, aligned, and integrated.

You may find that your organizational structure evolves the further you get off the ground.

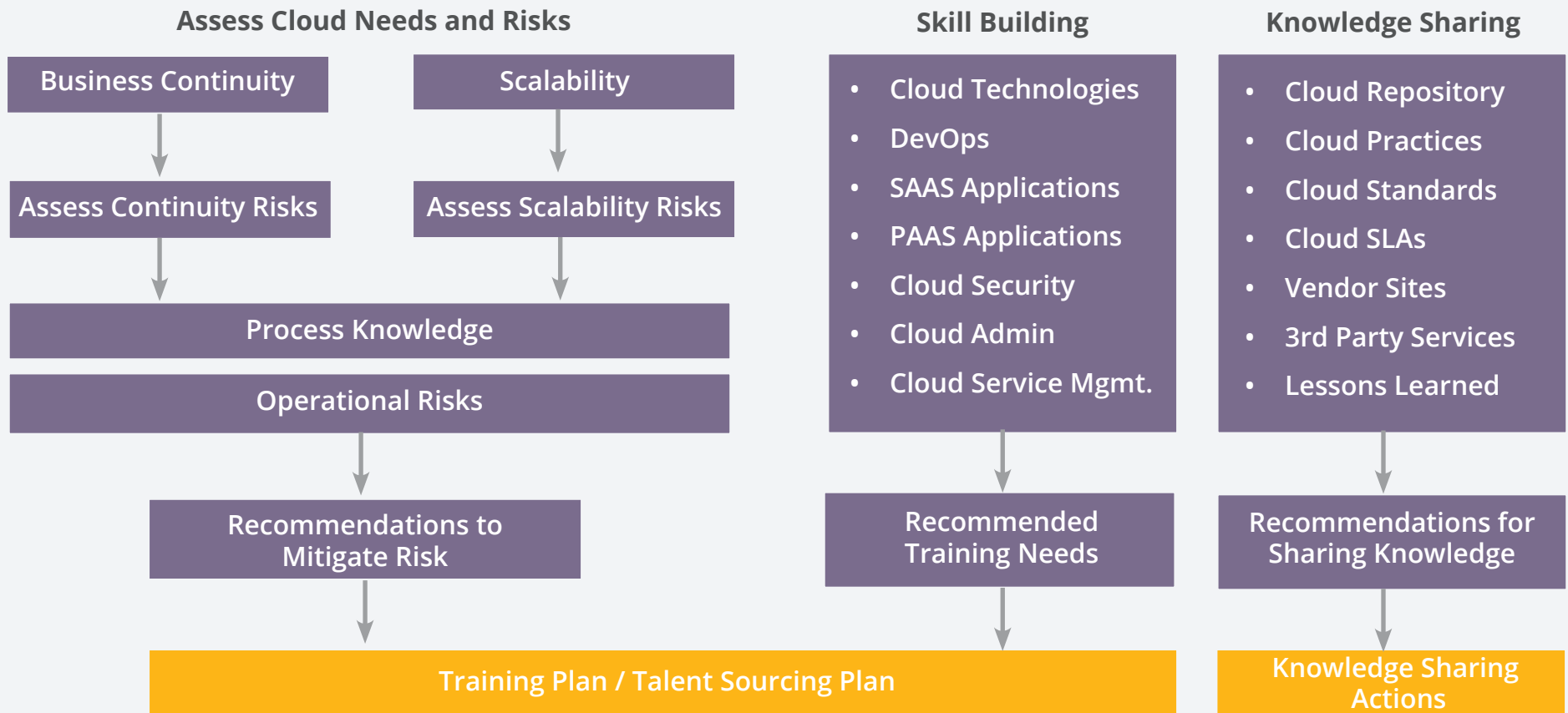


3 - EDUCATE YOUR CREW

Once you have everyone on board and the roles defined, it is important that you build your crew's cloud skills to ensure a successful transition.

Cloud skills need to be acquired internally and externally, taking into consideration what skills are needed today and in the future. Project managers must be aware of any current skill gaps and anticipate the most cost-effective means for filling these needs.

CLOUD TALENT ACQUISITION MODEL





Final Thoughts on Cloud Transition

During recent work with clients, we have learned what it takes for a cloud transition to soar. At World Wide Technology, their cloud transformation not only was an IT success, but also a people success.

[Read the client story.](#)

Conclusion

So you've decided to take the leap and make a migration to the cloud. But whether you're transitioning to cut costs, ramp up security, or tap into new business, there is a lot to remember before you buckle up and begin your journey.

In this guide, we covered how to prepare your business for take off: from learning how to share control with a cloud provider and avoiding data and security leaks, to seeing the cloud cost savings and getting your crew onboard with change.

Once you're safely off the ground, you'll want to shift your focus to using the cloud to accelerate innovation. Taking advantage of machine learning or voice and image recognition is so much more accessible today - and not just for company giants like Facebook or Tesla.

We're seeing mid-market companies use cloud technologies such as:

- Internet of Things to improve patient outcomes by using beacons to measure bedside dwell times of healthcare caregivers.
- Machine Learning to predict employee retention by analyzing the likelihood of an employee either staying or leaving.
- Cloud Native Development to better manage customer engagement by speeding up development, controlling cost, and ensuring repeatability.

Whether it's artificial intelligence, chatbots, blockchain, or any of the other tools that platforms like AWS and Azure can enable for you, the cloud can extend your enterprise today.

Cloud Readiness Checklist

When it comes to a cloud transition, there is a lot to remember. Below is a checklist of steps to help you on your way.

Cloud Control

Are you outsourcing the ownership and maintenance of assets?

Do you have good security measures in place for outsourcing?

Are you using the cloud services to track vendor performance?

Cloud Security

Do you have a clear inventory of the cloud applications and connected devices in your enterprise?

Do you have data classified into tiers to evaluate security requirements?

Do you have an identity management process that includes SaaS tools?

Do you have adequate staff and tooling to actively monitor logs?

Do you have a clear acceptable use policy that includes the use of cloud for your organization?

Cloud Savings

Do you understand differences between inception costs, employee costs, and intangible costs?

Have you made a cloud budget? Important costs to consider:

- Server Costs -
 - Hardware: Server, Rack, Infrastructure, PDUs, ToR Switches
 - Software: OS, Virtualization Licenses
- Storage Costs - Storage Disks, HBAs, SAN/FC Switches
- Network Costs -
 - Hardware: Core/Aggregation Switches, Bandwidth
- IT Labor Costs - Server Admin, Virtualization Admin
- Facilities Costs - Space, Power, Cooling, Security
- Subscription fees
- Operational costs

Cloud Transition

Are your business and IT teams aligned and ready for the change?


Do you have proper communication methods in place to keep all teams up to date?

Have you defined key roles for the transition?

Do you have the right governance in place?

Have you defined processes for clear accountability?

Does your team lack any cloud skills needed to make a successful transition?



The cloud can take your business to new heights.
Together, we can make the journey.

Have questions?
Let's talk.

CentricConsulting.com

((CENTRIC))