[[1]](#footnote-1)

Project Proposal-Preparation for Migration to Cloud for Smaller Enterprise Businesses

Andrew Abbott, Nathan Mowat, and Tracie Scott

*Abstract*—The migration to cloud for Fortune 500 and other global entities is achieved by engaging with top consulting companies and experienced professionals from the cloud providers themselves. For companies for whom that level of support is out of reach, what are the most effective methodologies and best practices to assure a successful, non-disruptive transition to cloud? This paper outlines a playbook for a smaller Enterprise or SMB organization to migrate operations from on premise to cloud. Our discussion will present planning criteria for the move, technical migration strategies, risk mitigation strategies, and change management considerations.

*Index Terms*—TBD Enter key words or phrases in alphabetical order, separated by commas. For a list of suggested keywords, send a blank e-mail to [keywords@ieee.org](mailto:keywords@ieee.org) or visit <http://www.ieee.org/organizations/pubs/ani_prod/keywrd98.txt>

# introduction

F

or this project, we will interview migration leads from two companies currently engaged in migration planning to understand their concerns and explore how they have planned and prepared for the migration. We will compare offerings from top cloud providers to present a ‘buyer’s guide’, highlighting the availability of professional assistance. The team will conduct a literature review to collect best practices and methodologies reported for cloud migration both in scholarly papers and in respected professional journals. Our search will include publications from the last six months (May ’17 – ‘Sept 17). Based on the research, we will create a migration planning guide to provide a Do-It-Yourself reference tool for smaller Enterprise operations transitioning to cloud.

## What is Cloud Computing

According to the [Cisco Global Cloud Index](http://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf), cloud-based data centers will process 92 percent of enterprise workloads by 2020. Many sources state that any service provided over the Internet is a cloud service. However, that is not technically accurate as services were provided over the Internet for decades before the ‘cloud’ was recognized. The use of commodity hardware and virtualization to provide horizontally scalable services over the Internet distinguish cloud infrastructures from older approaches. Technically, services can still be offered over the Internet without the key traits that distinguish a true cloud offering from an older architecture, although that is becoming increasingly rare. Cloud-based services provide the following key traits.

[**Self-service provisioning**](http://searchcloudprovider.techtarget.com/definition/User-self-provisioning)**:** End users can spin up resources [on demand](http://searchitoperations.techtarget.com/definition/on-demand-computing). This eliminates the traditional need for IT administrators to provision and manage resources.

[**Elasticity**](http://searchcio.techtarget.com/definition/IT-elasticity)**:** Companies can scale up as needs increase and scale down again as demands decrease. This eliminates the need for massive investments in local infrastructure, which may or may not remain active.

[**Pay per use**](http://searchcio.techtarget.com/definition/metered-services)**:** Resources are measured at a granular level, enabling users to pay only for the resources and workloads they use.

**Workload resilience**: Cloud service provider offer redundant resources to ensure resilient storage and to keep users' important workloads running -- often across multiple global regions.

**Migration flexibility:** In theory, organizations can move certain workloads to or from the cloud -- or to different cloud platforms -- as desired. Because providers may have termination fees and moving large datasets and/or critical applications may be problematic, this trait may not be fully realized.

There are four general types of cloud architectures:

**Public Cloud:** Cloud computing resides outside an organization, applications may be open to the public, and users access resources over the internet. These environments are typically multi-tenant, meaning multiple customers may share compute, network, and storage devices. Examples: Amazon Elastic Compute Cloud (EC2), Google AppEngine, and Windows Azure Services Platform.

**Private Cloud:** is a cloud computing model operated only for one institution/organization. It can be managed internally or by a third party and hosted internally or externally. Access to applications is likely tightly controlled as data is proprietary and/or confidential to the organization. Examples: HPE, IBM, Oracle, RedHat, and NetApp.

**Community Cloud:** Different organization with same policy and requirement share a same cloud computing and this is called community cloud.

**Hybrid Cloud:** Combination of public, private and community cloud is called hybrid cloud.

## Why move to Cloud

The key traits that define the cloud also provide the key benefits for moving to cloud. Unlike traditional IT models, which may require weeks or months to provision new hardware and build a stack to support a new application, cloud providers make services available quickly and easily. For quick trials or to manage episodic peaks in demand, leveraging cloud may be cheaper than purchasing and provisioning resources that normally would not be fully utilized.

**Specialty Skills:** Especially for smaller organizations, leveraging cloud services alleviates the need to hire specialized IT resources. Services can be easily and quickly provisioned in the cloud without the need for experts and the infrastructure is maintain and upgraded by the service provider. In addition, the cloud providers frequently have access to the industry leading experts in security, networking, infrastructure, and application deployment that are unavailable to the majority of organizations.

**Focus:** Allows focus on core skills instead of IT…

**Simplicity:** Removes the complexities of maintenance, such as patches and upgrades, as well the need to stay abreast of the latest products and trends….

## Reasons to defer move to Cloud

**Cost:** While provisioning services in the cloud can be quick and easy, it may not be cost effective. Even the cloud providers caution against assuming that cloud services will be cheaper than traditional IT services. While that may be true for some use case, for on-going use cases, the cost is frequently higher. The benefits lie elsewhere as described above.

**Lock-In and Loss of Control:** Organizations fear ‘lock-in’. Once data is migrated, the cost, tangible and intangible, of migrating to a different provider may be prohibitive. Also, what happens if the provider goes bankrupt? Who owns the data, and any copies thereof. Can a legal entity gain access to data through the provider that would not be available if it were on-premise?

**Security:** Most cloud infrastructures feature a shared architecture. As services are provided, many of the details of that service that would be controlled by your staff become transparent or invisible. Where is backup data stored? What happens to the data on a disk when the disk is replaced? Could data that is legally required to remain in-country be backed up to a target across the border? How trustworthy are the provider’s employees that have access to hardware and services?

These are the concerns that keep organization leaders from embracing cloud providers. In the early days of cloud, these concerns were justified. However, at this point, the major providers have solutions to mitigate these concerns and are motivated to protect their client’s environments. Industry leaders are having financial success and their business models are sustainable.

# General Approach

Use one space after periods and colons. Hyphenate complex modifiers: “zero-field-cooled magnetization.” Avoid dangling participles, such as, “Using (1), the potential was calculated.” [It is not clear who or what used (1).] Write instead, “The potential was calculated by using (1),” or “Using (1), we calculated the potential.”

# inventory

Make a list of needs. For each need, consider the litmus test attributes that would inform a migration decision. A successful cloud strategy starts with application discovery and dependency mapping to obtain an accurate inventory of the diverse applications currently running in the datacenter. A real-time and accurate discovery process can be very time-consuming with thousands of applications across an enterprise, but it’s imperative to understand each application’s makeup in terms of:

Application type and version

Operating system version and patches

Server, storage and networking characteristics

Security profile and rules

Interdependencies

Performance

Utilization cycles

Application architecture is a prime indicator of if and how an application can be migrated to the cloud. The costs—in terms of IT manpower and teams across disparate data centers—to map thousands of applications can be a major Opex expense that ties up IT talent and resources. Not every application is a suitable candidate for [cloud migration](https://www.cloudvelox.com/cloud-migration-services/). Your enterprise is like most in that legacy applications are rarely retired and may have outdated hardware dependencies operating in different corners of the business. This can include legacy applications running on platforms like mainframe and AS400 computers. Other examples include:

Applications with intensive CPU and/or I/O capacity needs

Vendor application designs and licensing that lack the structure for a virtualized environment

Proprietary applications

While major public cloud providers, such as AWS, are constantly developing new instance categories, they will never extend to outdated legacy or proprietary applications.

However, for the applications suitable for re-hosting the ROI of rehosting is immediate and substantial with 40 to 60 percent of your enterprise’s application portfolio falling into this category on average. Generally, enterprises choose such applications as:

CRM

HCM

ERP

Ecommerce

Windows business applications

Linux and x86 workloads

These are often the initial workloads that enterprises migrate as mapping from the data center to cloud-based instances is more straightforward. Of course, the process of moving these prime rehosting candidates can be still fraught with challenges and there are many[factors to consider](https://www.cloudvelox.com/learn/cloudvelox-blog/10-critical-planning-factor-series-8-automated-vs-manual-cloud-migrations-whats-the-difference).

…..more more more

# Types of Providers

## Infrastructure as a Service

Infrastructure as a Service (IaaS) providers deploy customer applications on their servers. When considering IaaS, it is important to consider service-level agreements (SLAs) provided by the vendor which should outline availability, scalability, performance, and maintenance policies. Data portability, user control, and security are also necessary considerations in an IaaS deployment.

<https://www.cisco.com/en/US/services/ps2961/ps10364/ps10370/ps11104/Migration_of_Enterprise_Apps_to_Cloud_White_Paper.pdf>

## Platform as a Service

Platform as a Service (PaaS) is an option for enterprises seeking to migrate applications that are based on standard platforms. The same considerations mentioned for IaaS are also necessary for PaaS

## Software as a Service

For some types of application, a Software as a Service (SaaS) based alternative may be desirable. In such a case, rather than an application migration, a SaaS option is a replacement of an existing application and it is the data that may need migration. Removing the need for management of the application and infrastructure has cost saving potential and allows resources to be focused on the core competency of the business.

## Private Cloud

For the few applications that are compatible with cloud architecture but you elect not to move into a public cloud, private cloud is marked by the following four characteristics [3]:

1. Flexibility and scale which meet client demands.

2. Resource sharing among a large number of users.

3. Payment (by internal users) according to use of the services.

4. Use of technologies and internet protocol to access cloud resources

Plus, there are additional benefits of private cloud [14]:

A private cloud platform with quick application provisioning and flexible ‘charge back’ options, converts IT into a partner with all shareholders within the business.

By leveraging the right private cloud provider, successful businesses gain higher reliability and avoid costly downtime for their critical applications.

Leading organizations take advantage of the best private cloud management efficiency in order to know how their critical applications are operating and avoid issues that can lead to lost revenues.

By working with a private cloud provider, leading organizations are able to offload many of the complications and day-to-day tasks of running critical applications while the provider will work carefully to maintain performance and avoid downtime and other issues to meet negotiated support levels.

Note that a private cloud can be provided in different configurations. A private cloud can be provisioned and managed exactly as a public cloud but on dedicated network, compute, and storage resources. Conversely, for organizations who have security concerns that prohibit deployment in a shared datacenter, the private cloud approach can be deployed using on premise resources and application management software. Within that, some offerings, like NetApp, focus on creating easily managed paths to the public cloud, while others, like HPE and IBM, are enabling their clients to offer the full public cloud experience from within the client’s data center to internal stakeholders, including the ability to “invoice” divisions/departments by utilization and to provision projects quickly on shared infrastructure. In short, there are a range of offerings in the marketplace.

All the various offerings are characterized by their own kind of risk. According to AWS, the deployment of resources on-premises, using virtualization and resource management tools, doesn’t provide many of the benefits of cloud computing but is sometimes sought for its ability to provide dedicated resources [4]. In most cases this deployment model is the same as legacy IT infrastructure while using application management and virtualization technologies to try and increase resource utilization. Several sources pointed out that the on-premise configurations are more costly as the organization had to provide for periodic technology refreshes. On the other hand, on premise private cloud can offer all the benefits of public cloud while ensuring decisions around security remain firmly in the control of the organization [5].

## Migration Options

Having an array of providers means that there is an array of options for leveraging cloud resources. Success is dependent upon picking the right path for each need.

**Just data migration.** This is typically the correct choice for Tier 1 and 2 applications. If you choose to migrate your VM or vApp, it’s still going to be constantly changing. If it’s a Tier 1 application you won’t be able to afford a lot of downtime, so typically, we’ll recommend invoking some sort of replication. Replication is a complex, detailed subject in itself, but the key to understanding it is to identify the size of the data, the rate of change and the bandwidth between the source and target. As a general rule, if your rate of change is greater than or equal to your bandwidth, your migration will likely fail. That’s because the rate of change refers to everything coming in to the app, it’s gaining gravity as the rate comes in. The bandwidth is like the escape velocity it requires to get off the ground, or migrate. You need a high enough bandwidth to “overtake” that rate of change.

**Machine replication**. This is best for Tier 1 and 2 applications that can afford some downtime and it involves stack migration.  There is less configuring in this scenario, but there is more data migrating. Option two is best if you’re moving to an internal private cloud. You will be able to replicate the entire stack, because you have plenty of bandwidth to move stuff around. It’s important to note the portability of VMware-based technology, because VMware allows you to package the entire VM/vApp, the entire stack, into an OVF. The OVF can then be transported anywhere if you’re already on a virtualized physical server.

**P2V migration.** You typically see this for Tier 2 and 3 apps that are not already virtualized. The concept involves taking a physical app and virtualizing it. VMware has a VMware converter that does P2V, and it’s very easy to go from a physical to a private cloud using P2V. It is, however, an entirely different set of best practices, and you should do some extended research to make sure you have the latest updates, best practices and suggestions. In this option, there is no replication; however, those apps can be shipped off to a public cloud provider to run in the public cloud after being virtualized.

**Forklift Migration Strategy.** This strategy is particularly useful for 3-tier applications. If the application is latency sensitive, it is recommended to move the entire application and all of its parts to the cloud at the same time instead of one piece at a time. This would include the app, the data servers that it accesses, and the web service that it uses [95]. In the forklift strategy the bulk of the work lies in the configuration of IP addresses, security groups, and DNS to name a few. The application code can stay relatively intact with few alterations.

**Disaster Recovery.** A final path some companies take is to treat it as a Disaster Recovery (DR) scenario.  Setting up something to do basically replication from the physical to one machine to another. They choose to replicate the entire stack from point a to point b, and then click the failover button.

# Research and select providers

Forbes released an article discussing the criteria for selecting a cloud provider. They summarized the challenge as follows [6]: “By choosing the wrong cloud provider, companies can get locked into an expensive and painful ordeal. Some providers have draconian severance clauses that make it nearly impossible to move to another provider if needed. The most critical component to consider when choosing a cloud provider is how they protect and secure data both at rest and in flight. Understanding the cloud provider’s data ownership and sovereignty policies is one of the key decision points when choosing a provider.”

By restricting selection to the top providers, we are also mitigating the security risks. Comparing security documents for top providers revealed a remarkable similarity between the security capabilities and features described by each [ 7,8,9]. Along with a list of compliance with other protocols, all have PCI DSS compliance for credit card processing. However, AWS was the only provider who stated they have Level 1 compliance, reserved for merchants with the highest volume of transactions, over 6 million card transactions per year. All three acknowledge that the organization retains ownership of data. All three offer data encryption at rest and in flight. All offer a robust set of tools for controlling policy-based access by user groups and services, retaining data within geographic boundaries as required by some countries, and implementation of high-availability options for disaster recovery and non-disruptive operation.

## AWS

## Azure

## Service Now

## SaaS providers

## On-Premise Private Cloud providers

# Plan migration approach for each application

## DIY or not-DIY

The decision to use a professional service to manage the migration to cloud or to do it in house depends largely on the complexity of the migration. The process requires a deep understanding of the interaction between applications and the underlying infrastructure. Additionally, complex migrations require program management skills. Professional service providers bring both of these skill sets along with valuable experience.

## Test Pilot

Before you migrate everything over to the cloud, a proof of concept test pilot build should be completed. Essentially a scaled down version of your application should be built in the cloud for a couple reasons. The first is that you want to try out the cloud with data that you can play around with and isn’t critical to the application if you lose it. You can start and terminate instances as you need to and perform stress tests. The second is that you want to learn the ropes of the cloud provider that you have chosen. It doesn’t make sense to move your application and data into something that have no confidence in. Build that confidence by building a test pilot. A proof of concept pilot also helps with company support and buy-in. When all the steps and details have been ironed out, then proceed with moving the real app and data.

## Network Requirements

## Compute Requirements

Before migration, data should be collected on each application. This application profiling is used to determine the compute resources necessary when the application is migrated. The profiling should cover enough time to capture daily and weekly fluctuations and include CPU usage, memory usage, storage throughput, latency, IOPS, and network data.

## Storage Requirements

## Data Migration Method Requirements

When it comes to migrating the data, the “best” method changes with the size of the data. If your data is under 1TB you are able to send it encrypted online without too much difficulty or time delay. The issues arise when the data becomes larger. If you were to migrate 10TB of data over the internet using a standard 100Mbps connection, Product Manager at Google, Ben Chong, estimates the transfer would take 12 days [96]. If you scale this up to the petabyte level, the transfers would take multiple years. Data larger than 1TB and up to 30 TB should ultimately be stored in a single NAS appliances and shipped to the cloud provider. These appliances should be able to encrypt using either of 128-bit or 256-bit AES encryption[97]. They should also be configured with RAID so that the data is not destroyed or corrupted during transit. If you have more than 30TB of data you can ship multiple appliances to your cloud provider where they use large 10GB connections to download the data.

When the data starts getting into the petabyte scale, there are other data transfer options. AWS has a service called Snowball and Google Cloud has a service called Google Transfer Appliance. These services are similar in the fact that each company sends custom server racks that can live in your data center for a few days and create a mirror of your data. They are then transferred by 18-wheeler (in AWS’s case) to the cloud facility. This form of transfer can speed up the transfer process from weeks to days for extremely large data sources[95,96].

## Security

## Downtime

There are many forms of downtime to consider when using the cloud, from SLA’s to increased downtime due to multiple services, or from the quality of the service to whether or not it’s the cloud that is down or just your application. We’ll just focus on the downtime that takes place during the migration process. Depending on how the application is structured and how it is connected into the system there are circumstances where there would be zero downtime. This is down by launching your application on the cloud while keeping your production application still live, then synchronizing them together. Then you use automation to cutoff the old application and point your system to the newly created application.

One such tool that helps with this process is called CloudEndure[98]. This is a five-step process that begins with installing the CloudEndure software onto the machine that holds the application or servers that you would like to migrate. The CloudEndure software then gets pointed to the cloud service of your choice and it starts to clone your machine onto the new cloud server. This cloning process takes place behind the scenes and doesn’t require restarts or even any writing to disks, so it does not impact the performance of your production environment. It is also uses AES 256-bit encryption, so you can know that your data is secured in transit. Once the cloning process has been completed there is a testing phase that ensures that your application or data has migrated over flawlessly. The final phase is called a “Cutover”. This is the process where the CloudEndure software points users to the application on the cloud instead of the original one. This process allows downtime to be almost eliminated altogether.

## Other risks

## Operational Excellence

# Change Management

## Communication Plan

## New Processes

## New skills

# Operational Excellence

[95] J. Varia, “Migrating your Existing Applications to the AWS Cloud,” Oct-2010. [Online]. Available: https://d0.awsstatic.com/whitepapers/cloud-migration-main.pdf. [Accessed: 2017].

[96]B. Chong, “Introducing Transfer Appliance: Sneakernet for the cloud era,” *Google Cloud Platform Blog*, 18-Jul-2017. [Online]. Available: https://cloudplatform.googleblog.com/2017/07/introducing-Transfer-Appliance-Sneakernet-for-the-cloud-era.html. [Accessed: 22-Nov-2017].

[97] New Tech ForumBy Howard Young,InfoWorld|Jul 26, 2017About | Emerging tech dissected by technologists and H. Y. I. W. J. 26 2017, “Best practices for migrating data to the cloud,” *InfoWorld*, 26-Jul-2017. [Online]. Available: https://www.infoworld.com/article/3211244/cloud-computing/best-practices-for-migrating-data-to-the-cloud.html. [Accessed: 22-Nov-2017].

[98] “Live Migration,” *CloudEndure*. [Online]. Available: https://www.cloudendure.com/live-migration/. [Accessed: 27-Nov-2017].

1. This paragraph of the first footnote will contain the date on which you submitted your paper for review. It will also contain support information, including sponsor and financial support acknowledgment. For example, “This work was supported in part by the U.S. Depart­ment of Com­merce under Grant BS123456”.

   The next few paragraphs should contain the authors’ current affiliations, including current address and e-mail. For example, F. A. Author is with the National Institute of Standards and Technology, Boulder, CO 80305 USA (e-mail: author@ boulder.nist.gov).

   S. B. Author, Jr., was with Rice University, Houston, TX 77005 USA. He is now with the Department of Physics, Colorado State University, Fort Collins, CO 80523 USA (e-mail: author@lamar.colostate.edu).

   T. C. Author is with the Electrical Engineering Department, University of Colorado, Boulder, CO 80309 USA, on leave from the National Research Institute for Metals, Tsukuba, Japan (e-mail: author@nrim.go.jp). [↑](#footnote-ref-1)