Thomas Duryea
LOGICALIS

Business and technology working as one

Selecting the right Cloud

Three steps for determining the most appropriate Cloud strategy

Selecting the most appropriate cloud model can be a challenging process for organisations and IT executives tasked with leading the project. This guide leads you through the three key steps you should take to:

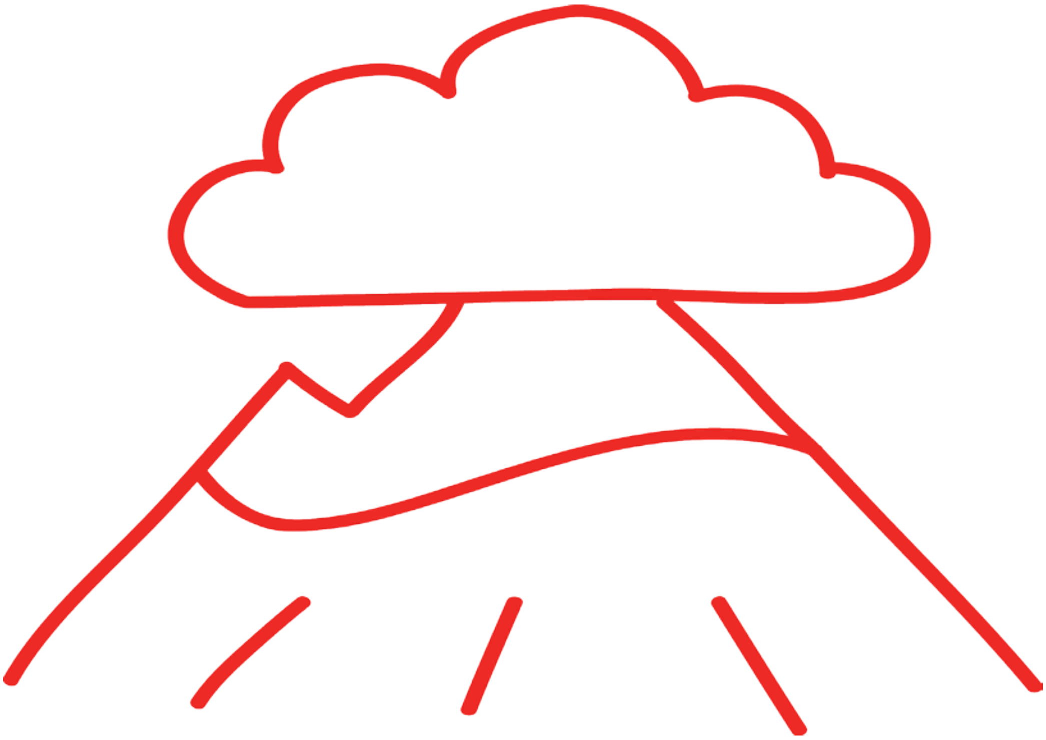
1. Assess your workload and select the most appropriate cloud model.
2. Understand what you should look for in a cloud provider
3. Ensure your cloud provider's migration methodology stacks up!

Why Cloud?

Businesses and enterprises have quickly realised the power and efficiency of cloud computing. The ability to deploy servers rapidly, scale them elastically and largely eradicate upfront cost has made Infrastructure as a Service (IaaS) attractive to both new and established businesses.

Organisations are seeing an increase in business demand for IT, but flat or declining IT budgets, creating an increasing gap in the provision of IT services. Cloud services are increasingly being used to close this gap, by reducing the cost of IT services and reducing or eliminating the administrative overhead of data centre administration.

However, many organisations are seeking validation of their strategy or assistance in moving workloads from a traditional on-premise data centre architecture to a private, public or hybrid cloud model.



1. Assessing your workloads

When looking at migrating production workloads to Cloud, it's important to recognise that not all clouds are created equal. Understanding these differences is critical as each Cloud drives unique requirements and suits specific workloads. In addition to different cloud models there are two "flavours" of Infrastructure as a Service (IaaS) models:

- → **Commodity IaaS** is intended for "cloud applications" where the application itself is distributed across nodes and also distributed across multiple availability zones for redundancy.
- → **Enterprise class IaaS** is intended for enterprise applications, with the cloud infrastructure designed for performance, with redundancy and high availability.

Typically, Enterprise Class IaaS clouds are most suitable for traditional workloads when reliability is required and expected. The approach is to protect the entire cloud, by providing a reliable hardware platform, high performance and site redundancy capability.

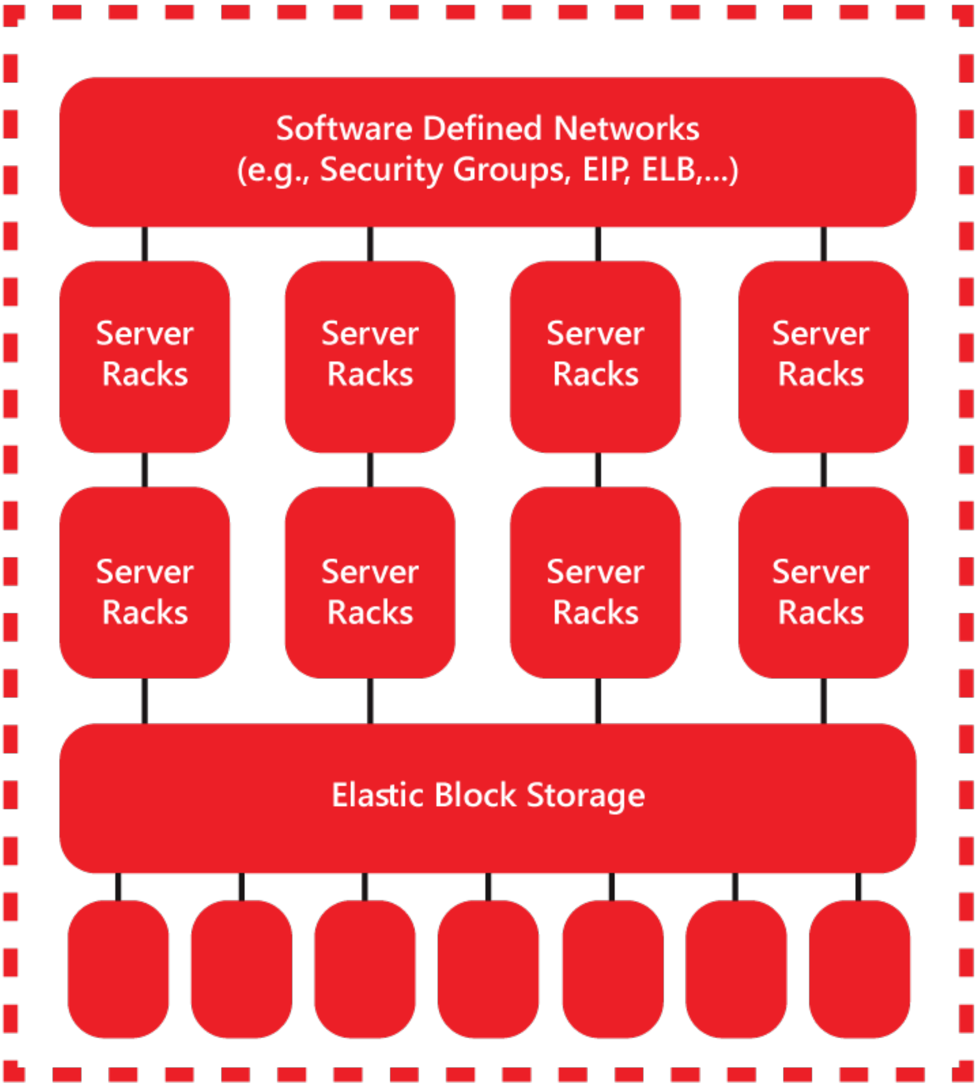
Conversely, Commodity IaaS clouds are built for distributed workloads. Infrastructure failure is expected and applications are designed to withstand this. Applications are built for multi site redundancy across zones.

> "When the CIO issues the simple directive 'Move some applications to the cloud', architects face bewildering choices about how to do this, and their decision must consider an organisation's requirements, evaluation criteria, and architecture principles."
>
> – Richard Watson, Research Director at Gartner

The Commodity IaaS concept

Application need to be architected from the ground up in order to take advantage of commodity clouds. In general, traditional and legacy applications are not generally suited for hosting in a commodity cloud and in many cases, will need to be re-written (or a lower level of availability and performance accepted). Applications can't rely on the infrastructure and they need to incorporate redundancy and high availability mechanisms.

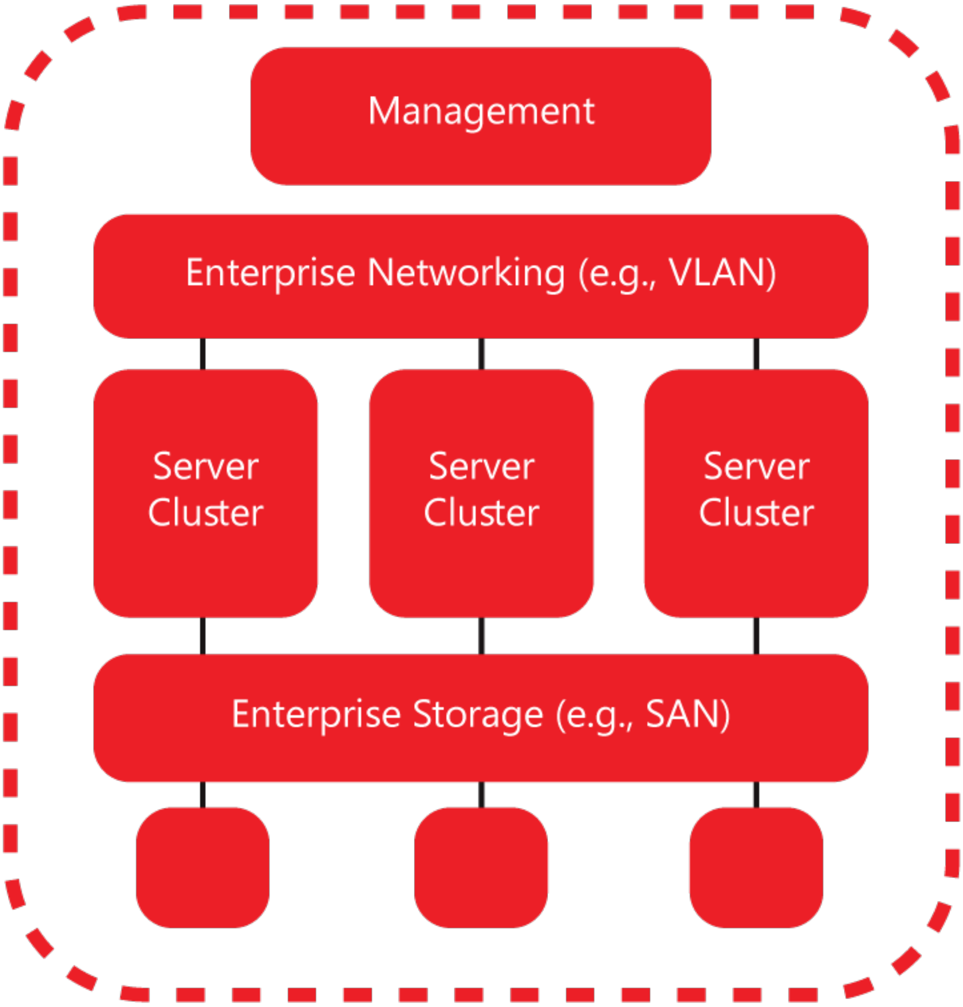
- Intended for "Cloud applications" (Web-scale applications)
- Designed for scale
- Lack of high availability in Zones / POD's (No guarantee on zone reliability)
- Applications to be designed to handle node level failure
- Applications required to be distributed across availability zones for redundancy



The Enterprise cloud concept

Traditional applications run reliably on an enterprise cloud – whether it's an on-premise (private) cloud or a public (multi-tenant cloud platform. An enterprise cloud provides high availability infrastructure to support applications and to provide redundancy through replication. This approach provides greater flexibility and should not require any re-architecting of the existing IT environment.

- Intended for "Cloud applications" (Web-scale applications)
- Designed for scale
- Virtual Machine (VM) failure is a normal state
- Lack of high availability in Zones / POD's (No guarantee on zone reliability)
- Applications to be designed to handle node level failure
- Applications required to be distributed across availability zones for redundancy

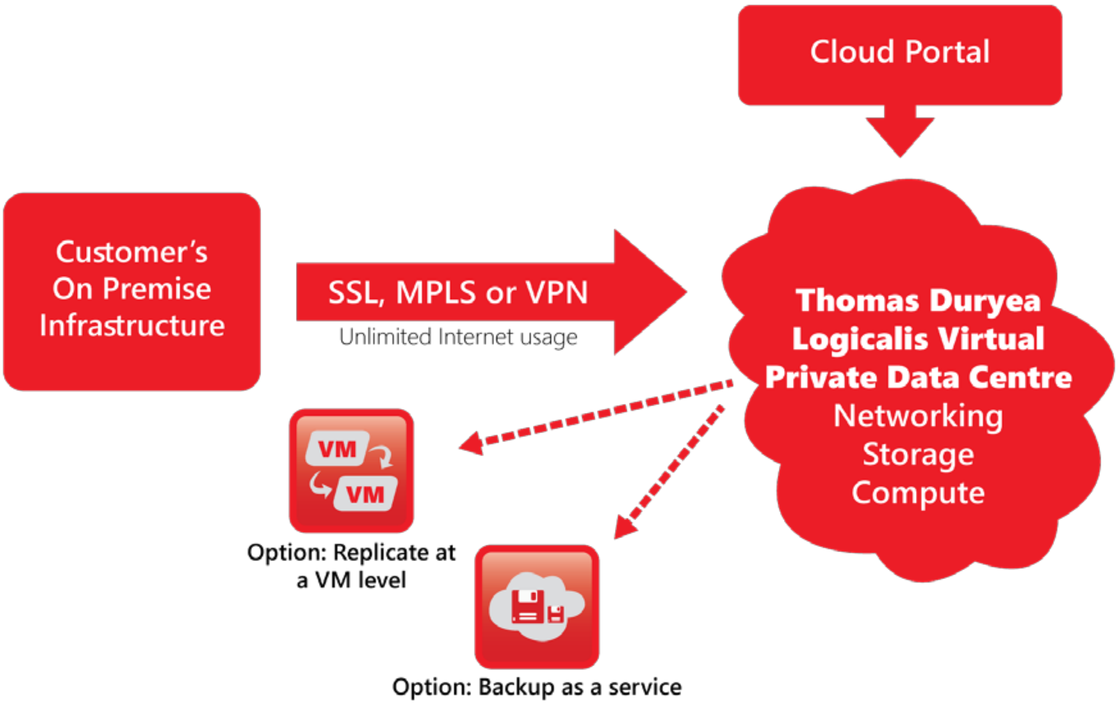

Management
Enterprise Networking (e.g., VLAN)
Server Cluster
Server Cluster
Server Cluster
Enterprise Storage (e.g., SAN)

Thomas Duryea Logicalis Virtual Private Data Centre: Enterprise cloud extended

Thomas Duryea Logicalis' cloud offering extends the Enterprise IaaS concept: the Thomas Duryea Logicalis Virtual Private Data Centre is an Enterprise IaaS offering that provide a dynamically configurable pool of resources isolated through a range of virtualisation and security technologies, making it a virtual single-tenant architecture dedicated to each customer.

The Thomas Duryea Logicalis VPDC extends the enterprise cloud model to include:

- Single pane of glass management one application to manage cloud or on-premise assets with rich service management)
- Self-service VM Replication (DR) integrated into the core platform (allows customers to choose nominated VMs to be replicated to a Thomas Duryea Logicalis secondary zone)
- Cisco Virtual Context Firewall (can be managed by Thomas Duryea Logicalis or customer)
- Self-service portal allowing customers to design their preferred network / security architecture using VLANs and / or Virtual Networks
- Integrated backup providing configurable retention periods
- Support for IPV6.


Cloud Portal
Customer's On Premise Infrastructure
SSL, MPLS or VPN
Unlimited Internet usage
Thomas Duryea Logicalis Virtual Private Data Centre
Networking
Storage
Compute
VM
VM
Option: Replicate at a VM level
Option: Backup as a service

> "Thou must remember that the onus is on the business (ie. the cloud customer) to ensure that the cloud provider used complies with local laws – local being where the cloud provider, and or the data, is being stored."
>
> – Cyberspace Law and Policy Centre at the University of New South Wales' Faculty of Law from *Data Sovereignty and the Cloud: A Board and Executive Officer's Guide*

2. Seven characteristics to look for in a cloud provider

The second key step in a successful cloud migration is the selection of a trusted provider.

Data Sovereignty

Public cloud services provide many benefits including services that can be provided from anywhere in the world and potentially from many locations. But this advantage can create concerns from a privacy perspective, as data placed outside of the location that the service is delivered can create difficulties for many organisations.

Some cloud provider contracts may specifically allow the provider to transfer data globally, or at least to the countries in which the provider has facilities. Thoroughly review any potential cloud contract to ensure that it aligns to your data transfer and location preferences or policies.

If your preference is for data to be kept locally in Australia (particularly in light of the Privacy Amendment Act) then seek Cloud providers that maintain data in Australian data centres and/or agrees that the content will not be moved without notification unless required by law.

Data Sovereignty

Data Ownership & Transferability

Programming Interfaces

Service Level Agreements

Storage Capabilities

Network Capability & Bandwidth

Financial Stability

Data Ownership & Transferability

Data transferability on termination or expiry of cloud services is critical to ensure organisations can continue to operate unhindered. It may also affect your legal obligations such as those documented in privacy laws or corporate record keeping requirements. Therefore, it is absolutely key that organisations understand how the service provider meets these commitments and specifically what mechanisms are available to extract data effectively or equally you understand their position on data destruction.

Often data retrieval is undertaken by downloading the data remotely. In cases where large amounts of data exist, arrangements with the service provider may be necessary for the physical retrieval of the data. Organisations should make these arrangements with the Cloud provider in advance. If you think you may need assistance with the post-termination data extraction, it is good to understand what services the cloud provider can offer.

Programming Interfaces

Cloud computing providers expose a set of software interfaces or APIs that organisations use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring can all be performed using these interfaces. Furthermore, organisations and third parties often build upon these interfaces to offer other value-added services to their customers. The Cloud provider's APIs have authentication mechanisms in place to ensure that only authorised API calls are made to their systems.

Organisations can take advantage of a Cloud providers API's to further enhance and control the Cloud service, making for a better more efficient service.

"Bottom line, the SLA is your contract with the service provider and sets expectations for the relationship. It needs to be written to protect your cloud service(s) according to the level of risk you are prepared to accept."

– Dr Angel Luiz Diaz, Wired

Service Level Agreements

Service Level Agreements are a key concern as they define aspects of the cloud service including service availability. Service availability aims to provide a "guarantee" of the percentage of time the service will be operational and typically service credits are provided to the customer for a failure to meet this guarantee.

Many Cloud providers outline service credit calculations in their SLAs and also document exclusions where service credits don't apply including such areas as scheduled maintenance, force majeure events or upstream provided Internet services. There are also instances where cloud providers provide no evidence that service credits are available to all, rendering the service target meaningless.

Ensure you carefully review the Cloud providers SLAs ensuring they are well understood and align to the expectations of their business.

Storage Capabilities

As application workloads have differing performance characteristics you cannot expect all cloud content to be treated the same. Data storage is growing at a substantial rate and customers need to balance performance and cost based on their workload and data requirements. Ensure your Cloud provider supports different classes or tiers of storage to allow you to choose the most appropriate platform for your workloads. Base this on performance, frequency of use and /or data protection requirements. This ensures that workloads perform as expected in the Cloud, cost effectively.

Organisations should seek the ability to control not only the applications and connections from the device to the corporate environment, but to collect real time device usage information and selectively wipe corporate data from non-corporate devices as required.

> "If startup history tells us anything, it's that the majority of cloud services launched in the past few years won't be around forever. The fact that they just vanish into the ether makes the problem quite perplexing."
>
> – Derek Harris, GIGAOM

Network Capability

As network connectivity is so important in a Cloud computing environment you must understand the cloud network services that any prospective providers support.

- Do they provide network options for private network connectivity (in the form of MPLS or Ethernet purchased from the customer's choice of carrier)?
- Do they allow customers to use their own IP address ranges or allow Layer 2 services into the Cloud environment? Some providers may enforce secure access to management consoles, restricting access to VPNs or private connectivity.
- Reviewing the supported network options is key as it can have a sizable impact when integrating or migrating services from the customer's on-premise data centre into the Cloud service.

Financial Stability

A seventh aspect to consider – whether you are considering a short-term, long-term or strategic relationship with a Cloud provider – is the vendor's financial stability. You should not have to worry about the provider going out of business.

A smaller provider may be the subject an acquisition. An acquisition can cause significant changes in the direction of a business and may result in a service transition period if the merged companies consolidate their platforms. Take some time to research annual reports, financial statements and ask potential providers to back up their financial claims.

3. Assessing your provider’s cloud migration methodology

Once you have assessed your workload and done your due diligence to match a cloud provider to your selection criteria, it is critical to manage the risk of migrating to the cloud by taking the time to ensure your cloud provider has a robust migration methodology.

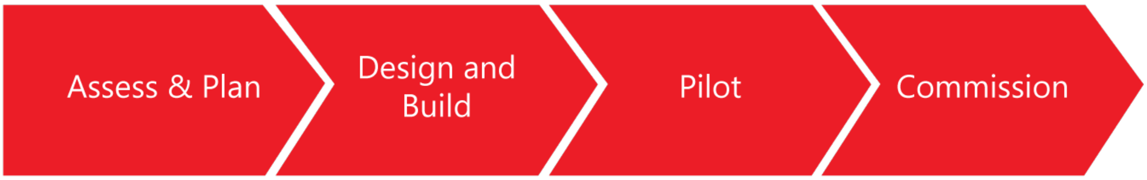
Inherently, migration to the cloud is a reasonable straightforward process as long as you have carefully planned approach.

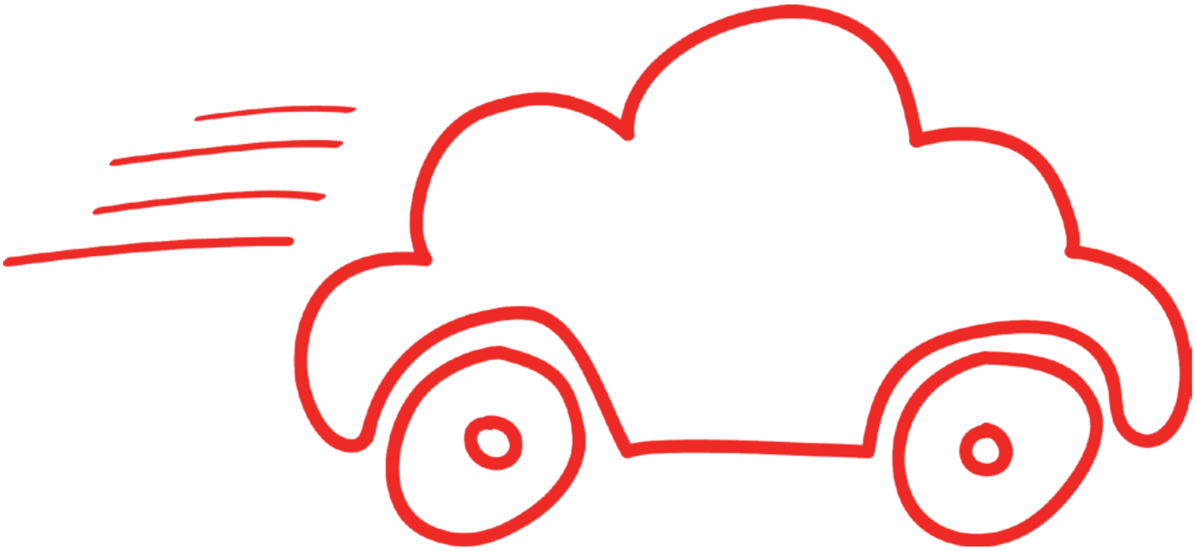
Assess and Plan

An incremental approach to cloud migration enables an organisation to “cloud-enable” its IT assets, without interrupting the businesses day-to-day operations. It is important to understand:

- → Drivers for migration – what are the priorities? (Is it driven by legacy technologies or a business driver, such as Capex pressure?)
- → Are there specific technical issues driving the requirements, such as Backup or Disaster Recovery?
- → What is the inventory of the current environment (a workload assessment will show the impact on the organisation of the migration).
- → What are the workloads, applications, dependencies, hardware and software configurations?

A full understanding of these points , typically through an assessment workshop, allows the organisation and Cloud provider to generate the best migration sequence. This ensures the benefits of cloud to the business can be delivered within an agreed budget and with a clear understanding of any risks involved.





Design and Build

The assessment determines the most appropriate plan for the design of the cloud migration plan, based on the destination workload profiles. The migration plan combines a specific sequence of actions, the human resources required and any support that maybe required from third parties during migration. It evaluates migration options for each specific workload and the location of the workload placemen including:

- Rightsizing the workloads
- The network design
- Application profiling
- Dependency mapping
- Data protection

The design and build phase should document the complete migration strategy for workloads migrating to the cloud. It is important to have clear communication of the planned cloud migration approach with all stakeholders.

Pilot

Pilot testing is a recommended approach, to mitigate any potential migration risk. It verifies that the services migrated or provisioned meet the business requirements and expectations. Piloting a UAT or Training instance of a service ensures critical business applications perform as expected in a cloud environment before migrating the production instances. Pilot testing also verifies the migration process, allowing for better planning of the commissioning phase.

Commissioning

At the successful completion of the Pilot a full-scale commissioning of the cloud program of works can be undertaken, including the implementation of any tools required for migration, workload configurations and network configuration.

.

A Cloud Business Case

Moving to the Cloud should realise significant cost savings, as well as enabling greater agility and reduced business risk. The use case below shows some of the benefits the Thomas Duryea Logicalis (TDL) Virtual Private Data Centre can deliver.

Engineering

The Business

A large Australian electrical engineering company.

Business Driver

A number of factors led the organisation to seek alternatives to their on-premise data centre infrastructure:

- Existing data centre was seen as a risk, with unreliable power and a single point of network connectivity
- There was no effective Disaster Recovery in place (and significant cost to the business as a result of any downtime incurred)
- Overextended IT team, which was challenged in delivering strategic projects, application development and IT operations

Use Case

Transitioning from an on-premise data centre infrastructure to TDL' Virtual Private Data Centre, including servers and applications. VM Replication between TDL' Sydney and Melbourne data centres provides Disaster Recovery.

Decision-making Criteria

The organisation considered a broad range of criteria in selecting the most appropriate Cloud provider:

- Strength of the services and consulting capabilities to help the organisation design, develop a migration strategy and move to the cloud
- Technical alignment to the requirements, including the provision of geographically separate active dat centres to provide true DR and a "single pane of glass" management capability
- Strategic alignment of the cloud services and roadmap to the organisation's future initiatives.

Benefits

The busines case for moving to Cloud showed a projected Total Cost of Ownership (TCO) reduction of 38% over three years, representing approximately $20K per month in savings. As well as reducing cost, the cloud solution significantly mitigates risk by providing greater availabiltiy then the on-premise infrastructure through the integration of DR.

Thomas Duryea Logicalis makes technology work for you.
Our expertise helps transform business operations – making them more flexible, efficient and productive. We deploy, manage and host secure, infrastructure that can increase agility, reduce risk through a consistent and repeatable framework, and cut operating costs by 20-50%. It's a result we've achieved time and again for both enterprise and government customers.

www.tdlogicalis.com.au
marketing@tdlogicalis.com.au