It's a Digital World

Cloud Fundamentals For Business

BizWyse®

By Linda Shave

It's a Digital World

Cloud Fundamentals for Business

Table of Content

Introduction

The digital revolution and the rate that new technologies are constantly evolving are impacting traditional business models. Cloud computing, big data, machine to machine, mobile devices such as tablets, smart-phones, wearable devices, and social networks are disrupting our traditional ways of working.

The key to competing in the global digital economy is business model innovation. Executives in all industries ought to be looking for new business rules, tools and techniques to exploit semantic web enabled technologies and big data (digital) assets in order to transform themselves into the next generation digital enterprise.

The new global economy requires a new way of working and a new way of thinking about the way we will work into the future.

About this guide

This guide is for all small business proprietors, business analysts, project managers, academics and students who are interested in knowing how they can capitalise on the next wave of business innovation.

'New tools, new rules' - few concepts have transformed business more profoundly than the digital revolution. The 21st century business manager is being forced to re-examine traditional management approaches and develop innovative strategies that are agile to continuous change.

Opinions, views and statements given in this book represent the author's views only and have been based on articles, presentations, discussion forums and workshops that I have written, delivered and participated in over the last ten years. They are not necessarily endorsed by any business management, academia or professional association.

Chapter 1

Cloud Deployment Models

- Cloud is not new
- What is Cloud?
- Five Characteristics of Cloud Computing
- What Are Cloud Deployment Models

• Cloud is not new

Cloud computing is not new the term 'Cloud' in its current context was introduced back in 1997 in a lecture by Ramnath Chellappa where he defined Cloud as a new "computing paradigm where the boundaries of computing will be determined by economic rationale rather than technical limits alone."

The concept is to provide a cloud-based platform that brings disparate groups of people, internal, external customers and partners together in order to collaborate, share resources, data, information, workflows and processes.

Cloud adoption is about maximising the value from shared resources, storage and data in order to create new value chains, products and services.

- ## What is Cloud?

The Cloud is not a physical thing it is a metaphor for the Internet. The Cloud in brief is a network of servers, and each server has a different function.

Some servers use computing power to run applications or deliver a service. For example, Adobe moved its creative services to the cloud. You can no longer buy the Creative Suite (Photoshop, InDesign, etc.) in a software packaged box. Instead, you must pay a monthly subscription fee to use each individual service. That is why it is now called the Adobe Creative Cloud.

The following link from *the American National Institute of Standards and Technology (NIST) provides a detailed explanation "What is Cloud":*

> What is "the Cloud"? The NIST Model: Part 1- A clear, concise definition.
>
> https://www.youtube.com/watch?v=6-BAH_I3bnY

- ## What is Cloud Computing?

Cloud computing refers to the underlying technologies and methods that are the building blocks of cloud services.

These include, for example, virtualisation, automation, self-service provisioning, usage-based service metering and charging, multi-tenant infrastructure and application architectures, web services, service oriented architecture (SOA) and application program interfaces (APIs).

The following link takes a closer look at - What is Cloud Computing:

What is Cloud Computing? - YouTube

https://www.youtube.com/watch?v=ae_DKNwK_ms

- ## Five Characteristics of Cloud Computing

What makes cloud computing different from software and other IT approaches? Unlike conventional solutions, such as installed software, cloud computing is uniquely defined by NIST as having the following 5 characteristics:

- **On-demand self-service**: individuals can set themselves up without needing anyone's help.
- **Broad network access**: available through standard Internet-enabled devices such as laptops and smartphones.
- **Location-independent resource pooling**: involves vendors using shared computing resources to provide cloud services to multiple customers. Virtualisation and multi-tenancy mechanisms are typically used to both segregate and protect each customer and their data from other customers.
- **Rapid elasticity (highly-scalable)**: consumers can increase or decrease the amount of available computer processing, storage and network bandwidth capacity at will.
- **Pay per use (measured service)**: consumers are charged fees based on their usage of a combination of computing power, bandwidth use and/or storage.

Source: *NIST (National Institute of Standards and Technology)*

Let us take a closer look at the essential characteristics of a Cloud as defined by *the American National Institute of Standards and Technology (NIST)*:

> What is "the Cloud"? The NIST Model: Part 2- The Essential Characteristics of a Cloud.
>
> https://www.youtube.com/watch?v=5zE72ABL3GE

• What are Cloud Deployment Models

Cloud deployment models come in four types these are:

- Community Cloud
- Private Cloud
- Public Cloud
- Hybrid Cloud

We will look at some of the features of each Cloud deployment model.

- **Community Cloud**: the cloud infrastructure is shared by several organisations and supports a specific community/communities.

Pros and Cons of Community Cloud

- Dedicated resource for a group of customers
- Managed and/or hosted internally or by a third party.

- **Private Cloud**: a private cloud (also sometimes referred to as an internal or corporate cloud) is cloud infrastructure operated for a single organization and is managed internally or by a third-party, and hosted internally or externally.

Pros and Cons of Private Cloud

- Resource dedicated to one customer
- Managed and/or hosted internally or by a third party
- More secure and expensive

- **Public Cloud**: a public cloud consists of a service provider offering resources, such as applications and infrastructure (server, operating system, network connectivity, storage, etc.) to an organization, a group of organizations and/or individuals or the general public over the Internet.

Pros and Cons of Public Cloud

- Resources shared by multiple customers
- Cost distributed across large customer base
- Service fee, by subscription, or pay-per-usage.

- **Hybrid Cloud**: a hybrid cloud environment can combine private or public cloud implementations that are connected together to deliver the benefits of multiple deployment models. Non-critical business activities can be performed using public cloud while business critical activities can be performed using private cloud.

  Pros and Cons of Hybrid Cloud

  - Flexible and scalable
  - Cost effective
  - Security
  - Customised combination of shared and dedicated resources.

- ## Some Hybrid Cloud Benefits for Consideration

There are many benefits of deploying cloud as hybrid cloud model these include:

- **Flexibility and Scalability** - offers both features of private and public cloud scalability and secure resources.
- **Security** - Private cloud in hybrid cloud ensures a higher degree of security.
- **Cost Efficiencies** – A public cloud is more cost effective than private cloud, therefore a hybrid cloud can provide business with cost savings.

- ## Some Hybrid Cloud Disadvantage for Consideration

Some of the disadvantages of deploying a hybrid cloud model for the business might include:

- **Networking Issues** - Networking becomes complex due to presence and up keep of both private and public cloud deployment models. These factors need to be considered.

- **Privacy, Security, Compliance and Governance** - It is necessary to ensure that cloud services are compliant with the business organisation's privacy, security policies and governance requirements.
- **Infrastructural Dependency** - A hybrid cloud model is dependent on internal IT infrastructure, therefore it will be necessary to ensure redundancy across data centers.

The following link takes a closer look at Cloud Deployment Models especially at the pros and cons and the features of a Hybrid Cloud Deployment Model

Cloud Computing Part 2: Cloud Deployment Models – By Nathan Bell, COO of Telkomtelstra

https://www.youtube.com/watch?v=UiahIcc5skI

Chapter 2

Cloud Delivery Models

- What are Cloud Delivery Models?
- Business Advantages for SaaS
- Pricing Models for SaaS
- Security and Privacy for SaaS
- Software-as-a-Service (SaaS) Driving Competitive Advantages

• What are Cloud Delivery Models?

Cloud delivery models are also referred to as Cloud Offerings. There are three primary cloud delivery models these are:

- Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

We will look at some of the features of each Cloud delivery model.

• Infrastructure-as-a-Service (IaaS)

IaaS can sometimes be referred to as Hardware as a Service (HaaS). This is the capability provided to the consumer in the provision of processing, storage, networks and other computing resources.

- IaaS is a cost effective solution for a company's computer systems infrastructure.
- Some IaaS vendors offer large 'full data centre' style infrastructure (e.g. IBM).
- Other IaaS vendors offer a more 'user centric' service providing data storage capabilities such as Dropbox etc.

• Platform-as-a-Service (PaaS)

The capability of deployment onto the cloud infrastructure consumer created applications.

- Provides both a platform and its solution stack as a service.
- Facilitates developing an application for use in the cloud. This means the application can be developed or customised without the cost and administration of having to buy the hardware and software in-house.

- **Software-as-a-Service (SaaS)**

The capability provided to the consumer is the use of the provider's applications running on a cloud infrastructure and accessible through a thin-client interface such as a web browser. E.g Gmail, Salesforce.

- SaaS is often referred to as 'on demand' software.
- Software and its associated content are hosted centrally rather than in-house.
- Accessed by users through their internet browser.

- **Business Advantages for SaaS**

Business want the flexibility of only spending money for what they need, when they need it.

- Business are moving from purchasing software application assets (**capital expenditure**) to SaaS application subscriptions (**operation expenditure**).

- SaaS offerings allow much greater flexibility in pricing structure. Business want the advantages of having the most current SaaS offering without the traditional costs of upgrades.

- Business want the advantages of having access to different SaaS offerings to be competitive, grow and be sustainable into the future.

- Business want the advantages of being able to on-ramp (take up) and off-ramp (drop/move) SaaS offerings to meet the changing needs of the business.

- Business want the advantages of being able to on-ramp (take up) and off-ramp (drop/move) SaaS offerings based on cloud service metrics and measures such as quality, access speed, usage and trust.

- **Pricing Models for SaaS**

Pay-per-user is the most popular SaaS pricing strategy.

- The advantage over traditional software pricing is that SaaS is available on almost all devices and does not usually incur separate charges for tablets, laptops, phones and other devices.

- Executives, management and the business need to consider ongoing budgets as cloud delivery models such as SaaS are a '**operational**' cost as there are no physical asset(s) and pricing models can change.

- Executives, management and the business need to consider business vulnerabilities for example:

    - How would we continue business if the Cloud deployment and/or delivery model and our information and data assets were unavailable for a period of time?
    - How would our risk change if all or part of the asset is handled in the Cloud?
    - What is our business continuity plan?

- **Security and Privacy for SaaS**

The following video by IBM Cloud Computing describes some of the security and privacy considerations that a business might take into consideration when considering Software-as-a-Service.

IBM Cloud Applications: Building Security and Privacy with IBM SaaS

https://www.youtube.com/watch?v=6zu2dtB8-wU

- **Software-as-a-Service (SaaS) – Driving Competitive Advantages**

The following link provides the following IBM study: Software as a Service (SaaS) drives competitive advantage for top companies.

https://www.youtube.com/watch?v=R9uSm7CB050

Chapter 3

Cloud Privacy, Security, Risk and Governance

- Cloud Governance
- What is Privacy and Security?
- Cloud Privacy, Security and Risk Governance
- What is Personal Data in the Digital Age?
- Risk Governance and Cyber-security
- What is Risk Management?
- Third Party Provider's Responsibilities and Accountabilities
- Storing Information and Data Assets in the Cloud
- Intellectual Property

• Cloud Governance

When you move business assets to the cloud, there is a good chance that you will lose control of your business assets to your cloud provider.

Cloud Governance refers to the decision making processes, standards and policies involved in the planning, architecture, acquisition, deployment, operation and continued management of a Cloud computing capability.

Executives, management and the business are still ultimately responsible and accountable for the governance, privacy, security and the risk management of business asset(s). This includes knowing the physical country location of personal data, information and data assets that have or will be transitioned to the cloud.

- ## Four Pillars of Governance for a Hybrid Cloud Environment

The following IBMInfosphere video outlines the four key pillars of information governance for a hybrid cloud environment.

IBMinfosphere

https://www.youtube.com/watch?v=IK9X_lwou1w

- ## What is Privacy and Security?

Privacy is very often united with security; however, they are two separate concepts.

- Privacy is about the appropriate collection, use and sharing of personal information whereas
- Security is about protecting such information from loss, unintended or unauthorised access, use or sharing.

- ## Cloud Privacy, Security and Risk Governance

Privacy as previously mentioned may have different meanings due to factors such as context, prevailing social standards, and geographic locations. Whilst this can make privacy challenging to address, the predominant concept persists that 'privacy' is the appropriate collection, use and sharing of personal information to accomplish business tasks.

Whilst privacy and security are two separate concepts, the importance of these two concepts intersect, for the consumer if their personal data is not safeguarded from loss, unintended or unauthorised access, use or sharing.

Risk governance for privacy and security of personal data should include precautions against external malicious breaches, inadvertent internal breaches and third party partner breaches.

- ## What is Personal Data in the Digital Age?

Personal data is described in privacy and information security circles as information that can be used on its own or with other information to identify, contact or locate a single person or to identify an individual in context.

- With the advent of rich geo-location data and associative analysis such as facial recognition the magnitude of personal data collected is greatly expanded and so are challenges for security in protecting such information from loss, or unintended or unauthorised access, use or sharing.
- Privacy challenges are further complicated if your business needs to comply with a range of conflicting regulations on privacy especially as privacy regulations can vary by region and country.
- Executives, management and the business should make certain that service level agreements are in place with the Cloud provider(s) for data protection.

- ## Risk Governance and Cyber-security

Effective risk governance and compliance are enablers to ensuring that the security risks framework of people, policies, processes and technology are consistent and measurable across the entire enterprise and across all suppliers of your Cloud deployment and delivery models.

Cyber-security is defined as the protection of systems, networks and data in cyberspace. Cyber-security will become a key component in the process for the identification, analysis and mitigation of risks to information and data assets.

Risk governance and compliance models need to adopt a pro-active perspective and include cyber-security into both the security framework and business strategies, policies and processes. There is a need to address evolving security challenges to protect the business against external malicious breaches, inadvertent internal breaches and third-party partner breaches.

- ## What is Risk Management

Risk management is a defined set of coordinated activities that enable the business to identify possible risks, analyse the consequences of the risk, treat, monitor, review and recognise

mitigation strategies to address the risk in order that the business can achieve its goals.

Risk Management:

- Is an integral part of all business processes and systems
- Is an essential part of decision making
- Is an essential part of the financial sustainability and business reputation
- Takes human and cultural factors into account.

Identifying Business Risk Tolerance

The ISO:3100:2009 framework provides you with a risk tolerance measurement tool to identify the consequences and impacts for the business reputation, process and systems, financial reputation and people.

ISO 31000:2009 Risk Management – Principles and Guidelines	Consequence				
People	Knowledge of systems and processes.	Knowledge of systems and processes.	Knowledge of systems and processes.	Knowledge of systems and processes.	Knowledge of systems and processes.
Reputation	Internal Review	Inspection required by internal committees or internal audit to prevent escalation.	Inspection required by external committees legal General's Office, or inquest, etc.	Major loss of reputation, seriously compromising major operations.	Significant asset destruction or other.
Business Process & Systems	Minor errors in systems or processes requiring corrective action, or minor delay without impact on overall schedule.	Policy, procedures and business processes occasionally not met or services do not fully meet needs.	One or more key accountability requirements not met. Inconvenient but not impacting service levels.	Strategies not consistent with governance/compliance requirements. Findings show service is fragmented.	Critical system failure, bad policy advice or ongoing non-compliance. Business severely affected.
Financial	1% of Budget or <$5K	2.5% of Budget or <$50K	> 5% of Budget or <$500K	> 10% of Budget or <$5M	>25% of Budget or >$5M
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
	1	2	3	4	5

ISO:3100:2009 framework

Benefits and Risks of Cloud Computing

The following video by Jesse Lindmar, Director of Computer Forensics for Sensei Enterprises, Inc. outlines What are the benefits and risks of cloud computing?

https://www.youtube.com/watch?v=aEHTscmW-eE

- **Third Party Provider's Responsibilities and Accountabilities**

It is essential that the products, information and services shared in the cloud are protected from security and privacy breaches. Make certain that appropriate steps are taken to ensure that agreements, policies and procedures for data protection, security and privacy are in place to counteract pilfering, fraud, and espionage attacks from within and outside of the Cloud.

Executives, management and the business need to be fully aware of the third party provider's responsibilities and accountabilities around how they are managing data protection, security and privacy risks.

Without full knowledge and control, your organisation may be at risk of sensitive data loss, data confidentiality, integrity, account hijacking and worst cyber-security breaches.

- ## Storing Information and Data Assets in the Cloud

Storing information and data in the Cloud is sometimes referred to as 'Cloud Vaults'. The security, privacy and protection of the Cloud vault may rest with your third party provider.

Executives, management and the business need to be fully aware of the third party provider's responsibilities and accountabilities around how they are managing security and privacy risks around your information and data assets.

You should make certain that information and data assets ownership and the geographical location of all storage sites are clearly articulated and that you can get your information and data assets back and/or migrate them to a new Cloud provider if needed.

- ## Intellectual Property

Intellectual property is another key concern when it comes to cloud services, in some cases cloud providers own the infrastructure or the applications, while the user owns the data, this demarcation is not always clear.

For example, open source software often combines data and code, and it is not always clear who owns the rights to what.

The following are some questions you might like to consider.

- Will we own are own information and data?
- Where will the information and data be located?
- How do we get our information and data back?
- How long will it take to get our information and data back?

Chapter 4

Cloud Implementation Strategy and Planning

- Cloud Implementation Strategy
- Cloud Implementation Planning
- Cloud Outsourcing Arrangement/ Contract Considerations
- Benefits of SaaS Deployment

• Cloud Implementation Strategy

The acquisition and implementation of a cloud services as previously identified are a form of **outsourced** shared services.

As such a Cloud implementation strategy and associated planning requirements for a Cloud solution are similar to that of an outsourcing arrangement/contract.

For Software-as-Service (SaaS) this might also include costing for transitioning from traditional on premises(on-site) licensing arrangements 'capital expenditure' to outsourced shared services 'operational expenditure'.

- ## Cloud Implementation Planning

The Cloud Implementation Planning phase details the high-level implementation timings, resources required, costing's, contingency plan and post implementation support.

The post implementation phase should also include processes for the periodic review of the cloud implementation contract.

- ## Cloud Outsourcing Arrangement/ Contract Considerations

The outsourcing arrangement/contract might consider the following:

- Corporate Governance
- Roles, Responsibilities and Accountabilities
- Risk Management and Assessment
- Assurance and Conformance
- Termination and Transition

Depending on your business you may need to consider other aspects into your cloud implementation strategy and planning. The following provide a brief overview of each category listed above:

Corporate Governance

In an outsourcing arrangement, information security should form part of the overall corporate governance of an organisation. Information security must be comprehensively addressed at all stages, including prior to the cloud contract being established, throughout the operation of the contract and during termination or transition of the contract.

Both the organisation and outsourcing provider's information security governance policies should be consistent and complimentary, ensuring the effective mitigation of both the risks and threats that may impact the delivery of the service covered by the outsourcing contract.

Roles, Responsibilities and Accountabilities

In any outsourcing arrangement, the establishment of clear roles, responsibilities and accountabilities between the organisation's executives and the outsourcing provider are essential.

In addition to the establishment of roles, responsibilities and accountabilities is the drafting, execution and monitoring of clearly articulated contractual arrangements for the provision of the service(s).

Risk Management and Assessment

In any outsourcing arrangement, effective risk management processes and detailed risk assessments are pivotal to the success of the outsourcing arrangement. A cloud based outsourcing arrangement may introduce additional threats that may need to be assessed these might include:

- The geographical location of information and business functions and the resultant legislative requirements that may be applicable;
- The privacy and integrity of the data within the cloud;
- The availability of the cloud service and business continuity provisions;
- The outsourcing provider's security and privacy processes and policy alignment to the organisation's internal security and privacy processes and policies.

Assurance and Conformance

A key component of effective information security management in an cloud outsourcing environment is the ability of the organisation to obtain assurance from the provider that risks are identified, have been managed, are being managed, and will continue to be managed.

Organisations should monitor providers for the management of assurance and conformance. Such monitoring might include:

- Regular information security management scorecards and reporting;
- Outsourcing provider commissioned information security audits;
- Standards certification (e.g. AS/ISO 27001); and
- Letters of assurance.

Termination and Transition

A cloud outsourcing contract can be terminated for a number of reasons including:

- Mutual agreement
- Due to underperformance
- Breach of security
- Breach of contract
- As a matter of convenience (such as pricing, service no longer needed)

The most important aspect of any termination (exit) plan is the return and protection of the organisation's data, materials etc. this is critical to achieving business continuity. In addition, ensure that your data is completely removed from the cloud provider's environment once the transition is complete, verified and the sign-off process is complete.

Cloud Fundamentals For Business

This guide is for all small business proprietors, business analysts, project managers, academics and students who are interested in knowing how they can capitalise on the next wave of business innovation.

Linda Shave, BizWyse®, 2016

BizWyse®
Linda.shave@bigpond.com