FIREBRAND

CompTIA

Cloud Essentials Certification

Courseware

Version 1.1

www.firebrandtraining.com

CompTIA
Cloud Essentials

3/27/2014

1

What is Cloud Computing?

3/27/2014

2

- Cloud computing refers to the ability to access computer resources that reside in flexible pools that can be adjusted to meet demand and where the physical location of such resources is immaterial

- Historically we have used the cloud symbol to represent the Internet without defining what is inside the cloud. In the case of the Internet it represents interconnected networks
- The cloud in cloud computing now represents servers, storage, applications, and data centre infrastructure that allows us to access resources in virtual environments in a flexible manner

- Internet based hosting services have been with us for a while but cloud computing goes beyond providing just a web server application to providing a complete environment replacing the traditional locally based resources.
- Cloud computing comes in several forms which will be described later but they all have common factors listed below

- Managed externally by a service provider – the cloud provider manages the service so the customer is no longer concerned with local issues around data centre provision.
- Developers only need to know what type of platform their applications are running on
- Hardware knowledge is less important – it is all provided and maintained remotely

- Flexible resource assignment – the resources used in the cloud can be increased or decreased on demand with associated costs adjusted accordingly, based upon consumption
- This allows organisations to add new applications with minimal startup costs and also deal with spikes in demand with increased capacity
- The resources used in the cloud come from a pool that is managed and allocated by the cloud provider

- Network accessible – because the services are now “in the cloud” they are accessible over the network and via network devices
- Service can be provided anywhere anytime from anywhere which can insulate the service from environmental threats and political turmoil. Services can be hosted from different locations in a way that is completely transparent to the user

- Sustainable – resources are provided to meet demand so during off-peak times power consumption can be reduced with environmental benefits
- Resources can also be moved to where there is extra power capacity rather than require additional power in a local centre

- Managed through self-service – resources can be added to and managed by the client with minimal difficulty
- If the contract allow, resources can be manipulated automatically without technical assistance

- Distributed application design allows for the various elements of an application to be hosted in different locations and to be moved as required without service interruption
- Cloud applications are typically connected using standard APIs and XML web interfaces

- The ability to move resources on demand provides for greater resilience against threats such distributed denial of service attacks (DDoS)

- Cloud computing makes extensive use of virtual environments where multiple virtual servers can be hosted on one physical server
- Virtual server resources can be adjusted by added additional RAM, CPUs and storage to increase the processing capabilities without the need for costly physical upgrades

- Cloud computing also allows the use of High Performance Computing (HPC) techniques using distributed processing across multiple virtual instances

Cloud Computing Technologies

- Workstation – the traditional workstation works equally well in cloud environments
- Thin client – the software runs on servers not the client so this maps nicely into cloud computing
- Mobile clients – because cloud services are predominantly web based we can now use smartphones and tablets to connect to cloud services
- Other cloud services – services can be blended at the back end with front end access being seamless

Cloud Models

Cloud Models

- Evolution from Virtualisation to the Cloud
- Traditional data-centre infrastructure starts with server virtualisation
- Represents an increase in overall virtualisation from storage and hardware to include all components of network infrastructure.
- On site requirements can transit to existing entirely in the cloud

Cloud Models

- Private Cloud
- A local private cloud resident upon hardware located in local data centre
- Running cloud infrastructure software
- Self service resource allocation and metering
- Still involves capital and operational costs

Cloud Models

- Hybrid Cloud
- Bridge local private clouds with other cloud offerings to create hybrid clouds
- Extend resource pool beyond local data centre
- Develop greater capacity for responding to peaks in demand
- Retain total control over data resources
- Capital expenses reduced

Cloud Models

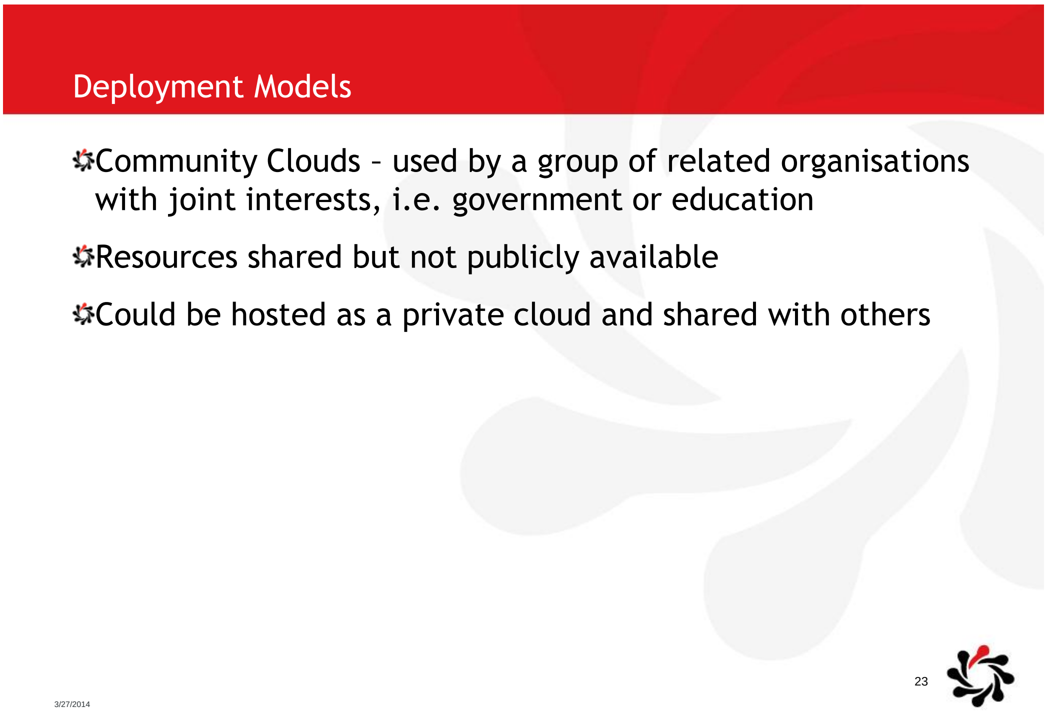
- Public cloud
- Externally provided environment
- Industrial scale cost efficiencies and hosting flexibility
- Mobility of hosting
- Green initiatives
- Capital expenditure now limited to client access technologies

Organisational Roles

- New organisational roles emerge as part of the change
- Capacity planners
- Network operation centre staff
- Vendor management staff
- Support desk staff
- Cloud architects
- Cloud service manager

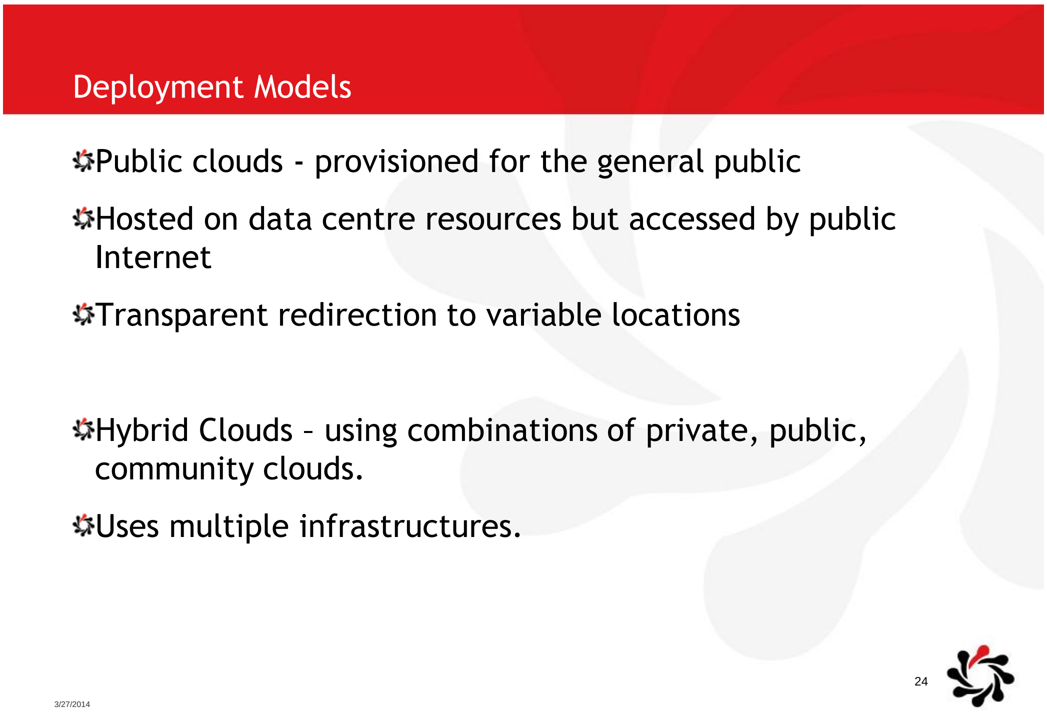
Deployment Models

- National Institute of Standards & Technology (NIST) documents four models for cloud deployments
- Private Clouds – provisioned for use by users within an organisation. Managed, owned and operated by the organisation. Reside on a private network managed by the organisation



Deployment Models

- Community Clouds – used by a group of related organisations with joint interests, i.e. government or education
- Resources shared but not publicly available
- Could be hosted as a private cloud and shared with others



Deployment Models

- Public clouds - provisioned for the general public
- Hosted on data centre resources but accessed by public Internet
- Transparent redirection to variable locations

- Hybrid Clouds – using combinations of private, public, community clouds.
- Uses multiple infrastructures.

Service Models

Service Models

- The services are represented in the form of a pyramid.
- Infrastructure as a service (IaaS) is the most fundamental service category, i.e., networking and storage
- Application developers use the services provided by Platform as a Service (PaaS)
- Users will consume the services provided by Software as a Service (SaaS)

Software as a Service

- Hosted software applications available through a web browser or thin client, usually indistinguishable to the user
- Examples include:

Microsoft Office 365

Pixir photo editor

Zoho CRM online

Kenexa HR solutions

Software as a Service

- Software apps are prebuilt and are usually limited to user personalisation
- User mobility and hardware replacement do not affect SaaS availability
- Additional business processes such as Business Continuity and DR are supported
- Resource sharing across timezones
- Green initiatives such as travel-free workers

Platform as a Service

- Platform as a Service (PaaS) expands the capability to customise application development
- Allows access to development tools
- Usually coupled to vendor technologies &languages
- Providers include:

Windows Azure

Google App engine

Rackspace

Savvis

Infrastructure as a Service

- Infrastructure as a Service (IaaS)
- Client has complete control over applications, languages and resources
- Sometimes referred to Hardware as a Service
- Can effectively eliminate local data centre requirements
- Providers include:

Amazon Web Services

IBM Cloud

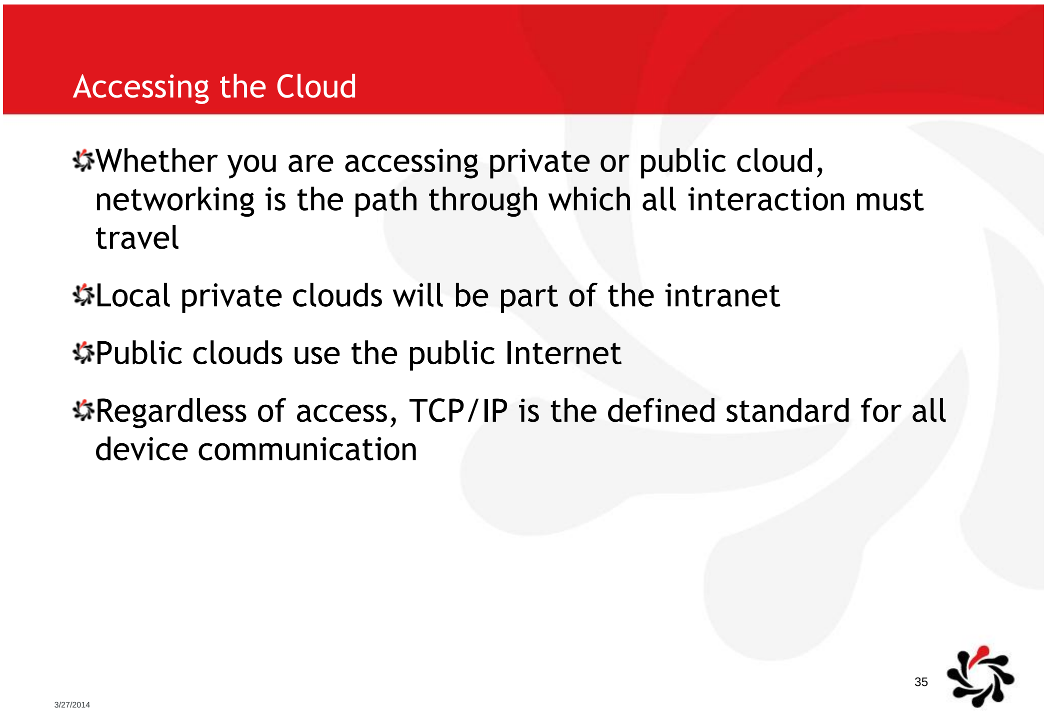
EMC2

Current Cloud Technologies

- Comparing traditional with Cloud
- Common desktop apps no longer require installation locally and the majority of features are available in cloud-based equivalents
- Web based services have the advantage of being accessible from machines without local installations of applications

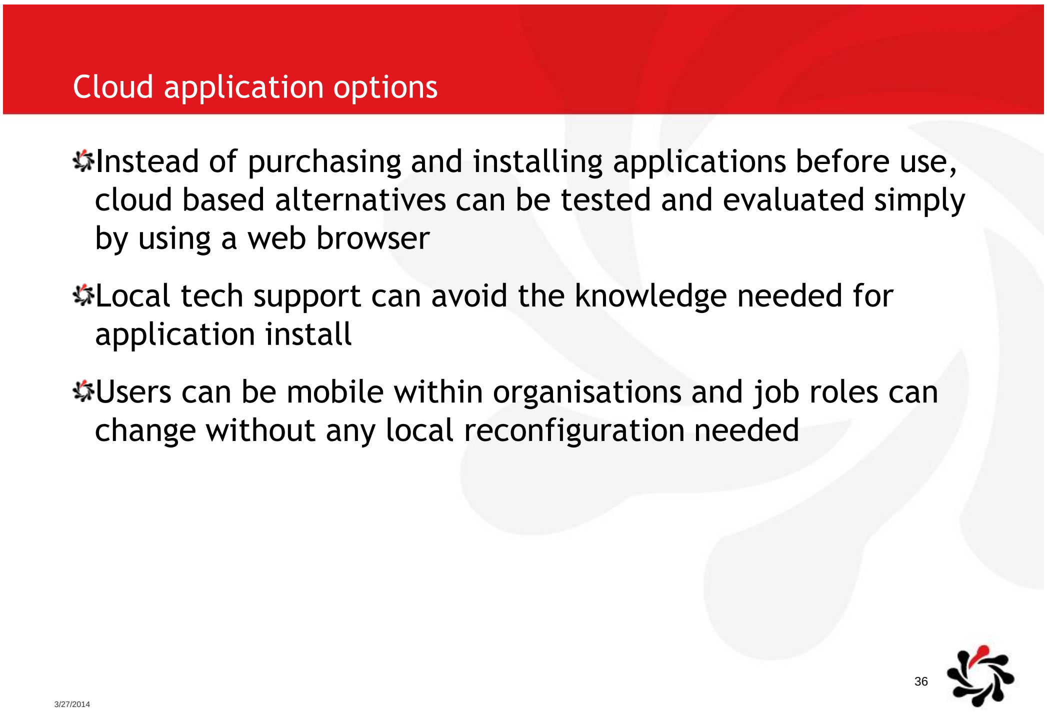
- Cloud based apps can be shared to other consumers with relative ease
- Fully featured audio/video production suites available to support multimedia
- Traditional apps no longer require the levels of technical support that was necessary

- New user interfaces such as Windows 8 allow for the transparent integration of cloud services alongside the traditional local resources installed on the workstation



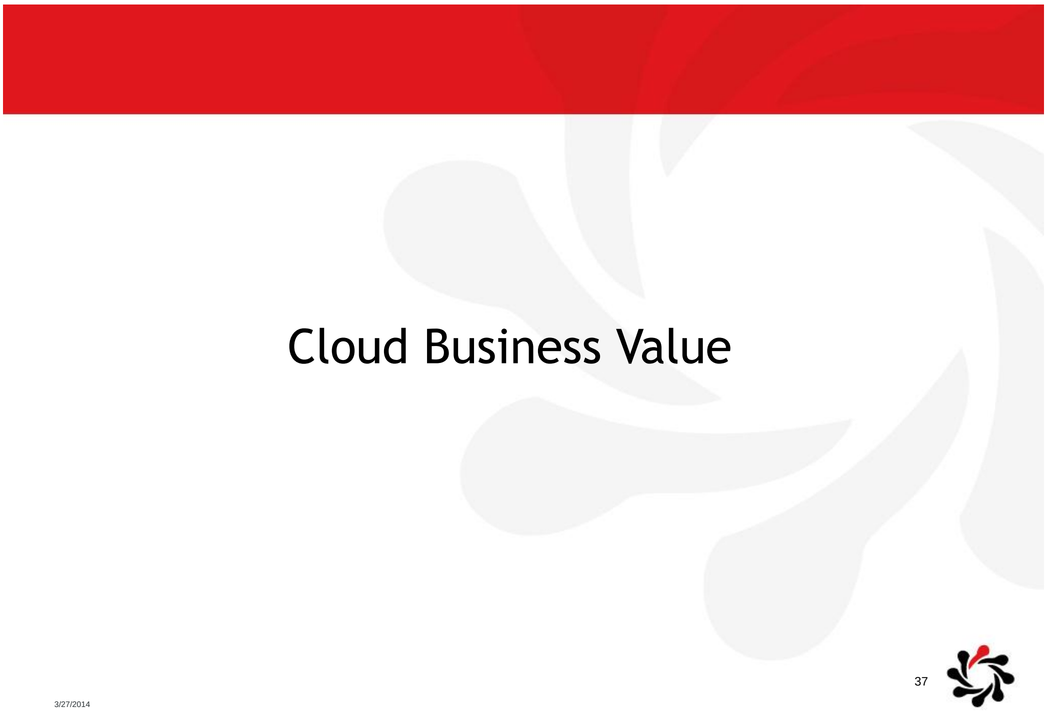
Accessing the Cloud

- Whether you are accessing private or public cloud, networking is the path through which all interaction must travel
- Local private clouds will be part of the intranet
- Public clouds use the public Internet
- Regardless of access, TCP/IP is the defined standard for all device communication

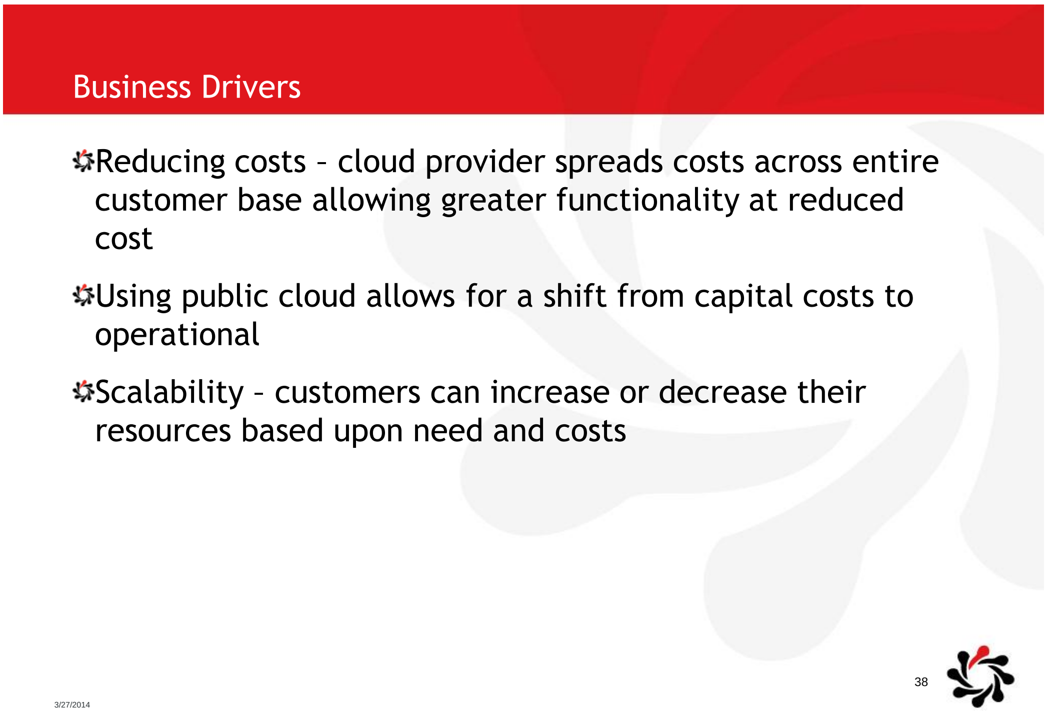


Cloud application options

- Instead of purchasing and installing applications before use, cloud based alternatives can be tested and evaluated simply by using a web browser
- Local tech support can avoid the knowledge needed for application install
- Users can be mobile within organisations and job roles can change without any local reconfiguration needed

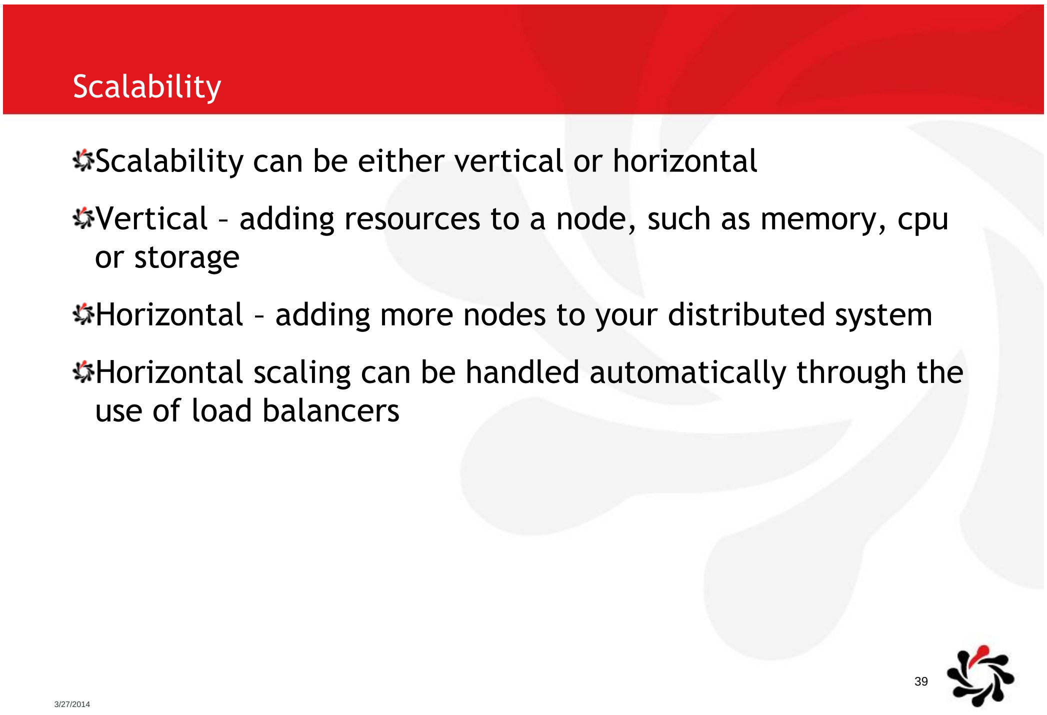


Cloud Business Value



Business Drivers

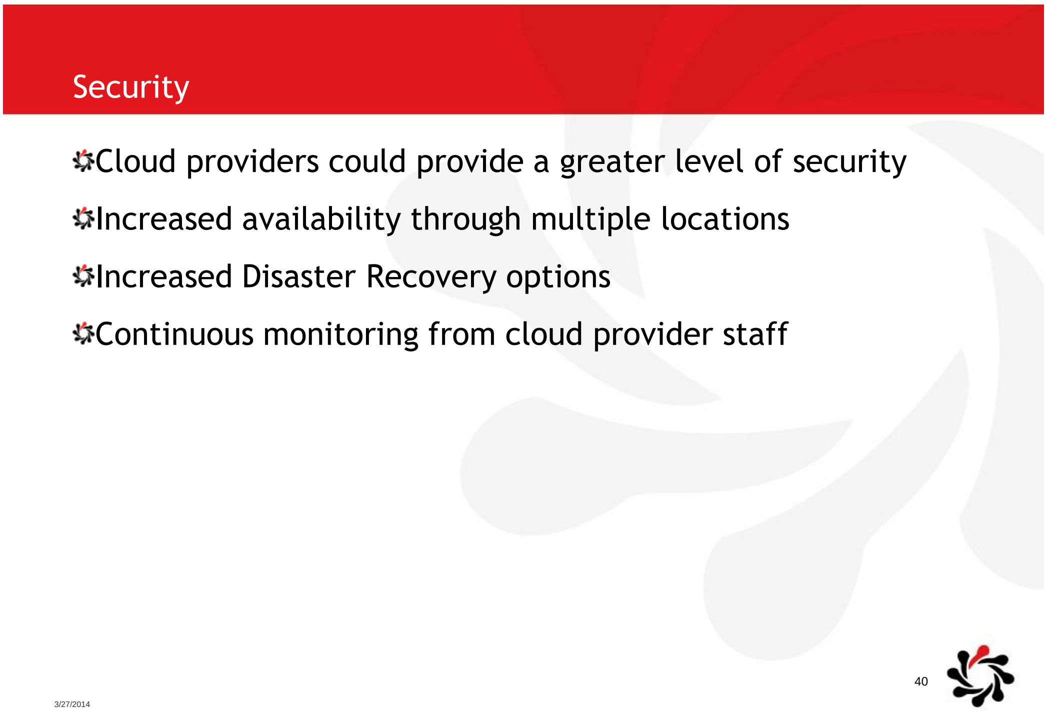
- Reducing costs – cloud provider spreads costs across entire customer base allowing greater functionality at reduced cost
- Using public cloud allows for a shift from capital costs to operational
- Scalability – customers can increase or decrease their resources based upon need and costs



Scalability

- Scalability can be either vertical or horizontal
- Vertical – adding resources to a node, such as memory, cpu or storage
- Horizontal – adding more nodes to your distributed system
- Horizontal scaling can be handled automatically through the use of load balancers

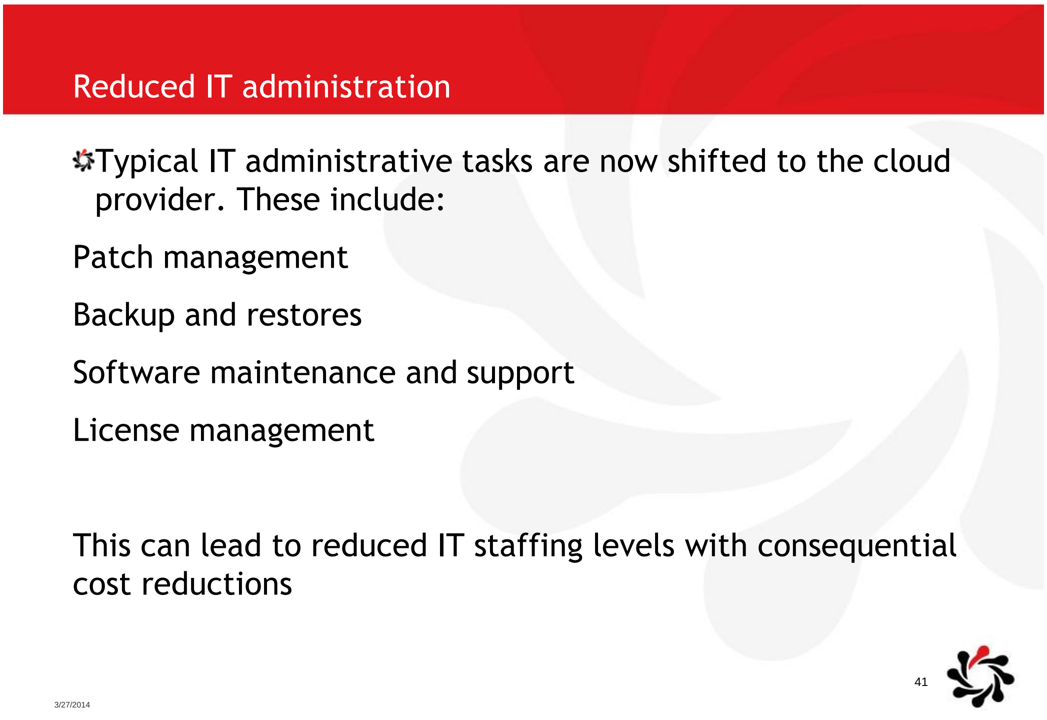
3/27/2014



Security

- Cloud providers could provide a greater level of security
- Increased availability through multiple locations
- Increased Disaster Recovery options
- Continuous monitoring from cloud provider staff

3/27/2014



Reduced IT administration

- Typical IT administrative tasks are now shifted to the cloud provider. These include:

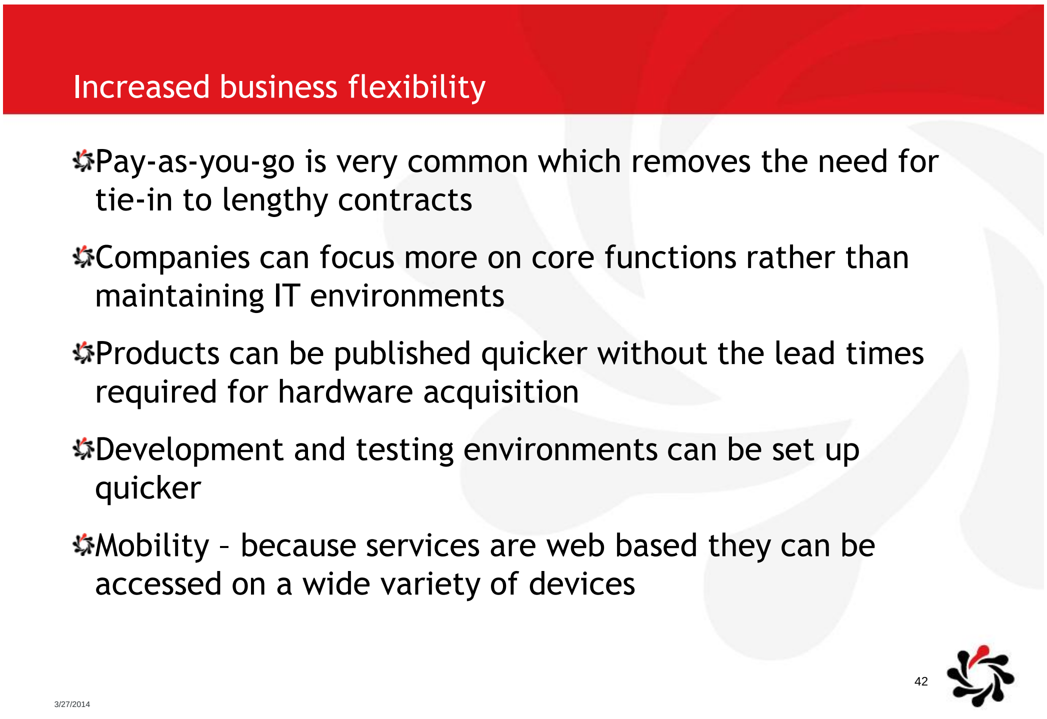
Patch management

Backup and restores

Software maintenance and support

License management

This can lead to reduced IT staffing levels with consequential cost reductions



Increased business flexibility

- Pay-as-you-go is very common which removes the need for tie-in to lengthy contracts
- Companies can focus more on core functions rather than maintaining IT environments
- Products can be published quicker without the lead times required for hardware acquisition
- Development and testing environments can be set up quicker
- Mobility – because services are web based they can be accessed on a wide variety of devices

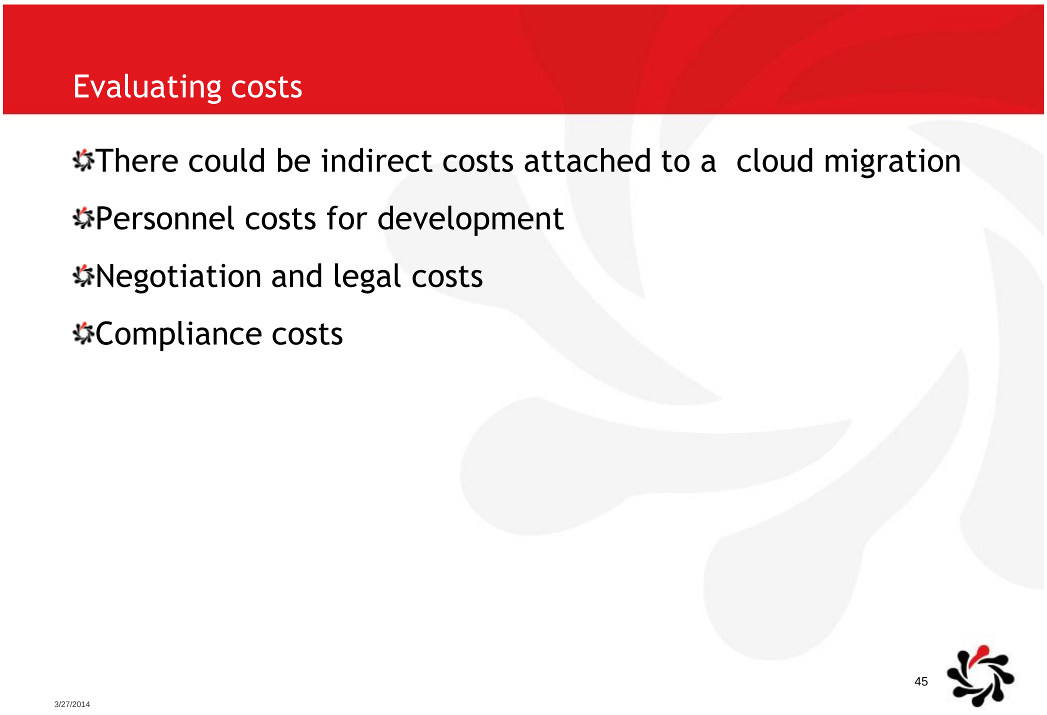
Business impact

- Moving to the cloud has elements of risk and uncertainty
- Before any migration the following steps should be taken:

1. The costs of the cloud should be evaluated
2. Identifying the value to the business
3. Which cloud model is most appropriate

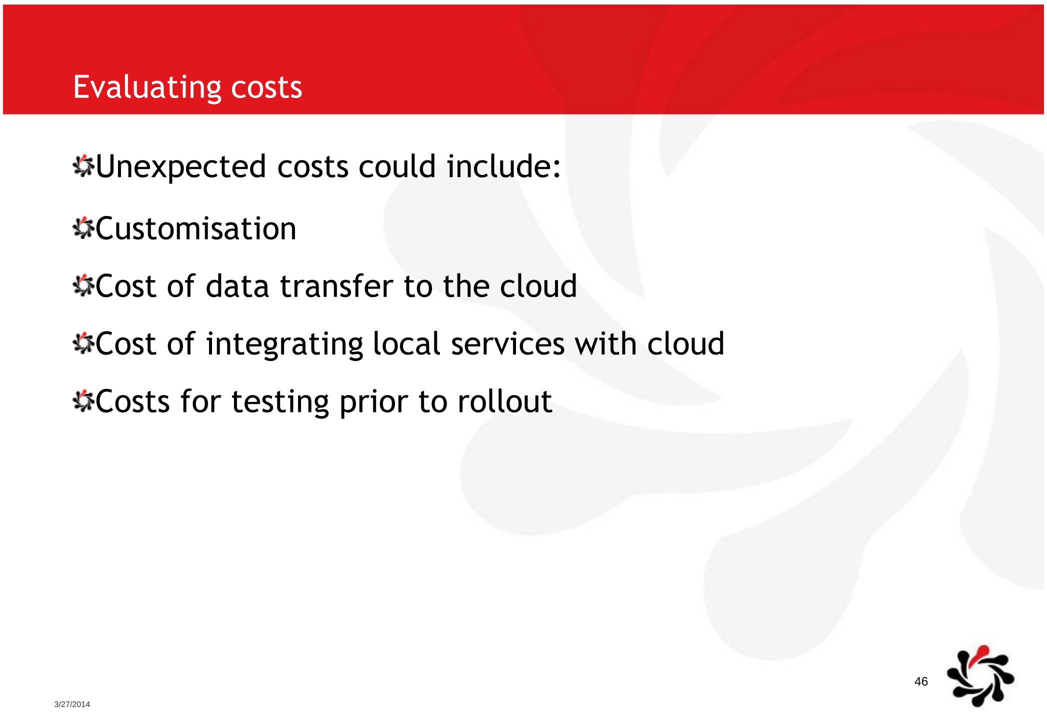
Evaluating cloud costs

- What are the direct costs of data storage and transfer?
- Are there additional costs associated with license and hardware procurement?
- What are the costs for bandwidth provision?
- Costs for increased availability and guaranteed resources



Evaluating costs

- There could be indirect costs attached to a cloud migration
- Personnel costs for development
- Negotiation and legal costs
- Compliance costs



Evaluating costs

- Unexpected costs could include:
- Customisation
- Cost of data transfer to the cloud
- Cost of integrating local services with cloud
- Costs for testing prior to rollout

Cloud Infrastructure Planning

Basic architecture

- Cloud networks should provide the following:
- Scalability – expansion to meet variable data and bandwidth requirements
- Resilience – network availability is critical
- Throughput – the network must support the ability for large quantities of data transfer
- Simplified management – using defined networking standards that can be easily managed.

OSI 7 Layer Model

- The OSI model is used to define network communications
- Each layer has specific functionality (as shown on next slide)
- Private cloud can use a mixture of Layer 2 and Layer 3 technologies

OSI 7 Layer Model

	Layer	Function
7	Application	Interaction with application software
6	Presentation	Data formatting
5	Session	Host-to-host connection management
4	Transport	Host-to-host data transfer
3	Network	Addressing and routing
2	Datalink	Local network data transfer
1	Physical	Physical Hardware

Layer 2 Cloud

- Using layer 2, all elements of the cloud share the same address space, i.e., the same subnet
- Interconnection through switches
- All IP and MAC addresses can share a common area
- Could be congested through CSMA/CD (collisions)

Layer 3 Cloud

- Cloud resources are interconnected through routers
- Segmenting the network using routers reduces the number of neighbours on a segment
- Allows widely separated subnets to exchange data
- Layer 3 can expand to a virtually unlimited number of hosts

Combining layers 2 & 3

- Using layer 3 routers to separate subnets along with layer 2 interconnections can provide virtual network connections
- This function can be provided by layer 3 switches and through the use of trunk connections between switches

Versions of IP

- The original version 4 is in widespread use but is being superceded by version 6
- Many cloud providers are implementing IPv6 because of it’s scalability
- IPv6 has the following benefits:

Reduced congestion through the removal of broadcasts

Improved routing capabilities with simplified addressing

Automatically generated addresses reduce conflicts

- Not all cloud providers can support IPv6 yet, something to be considered

Cloud Network Challenges

- The biggest problem for providers is delay or latency. This being caused by a range of factors:

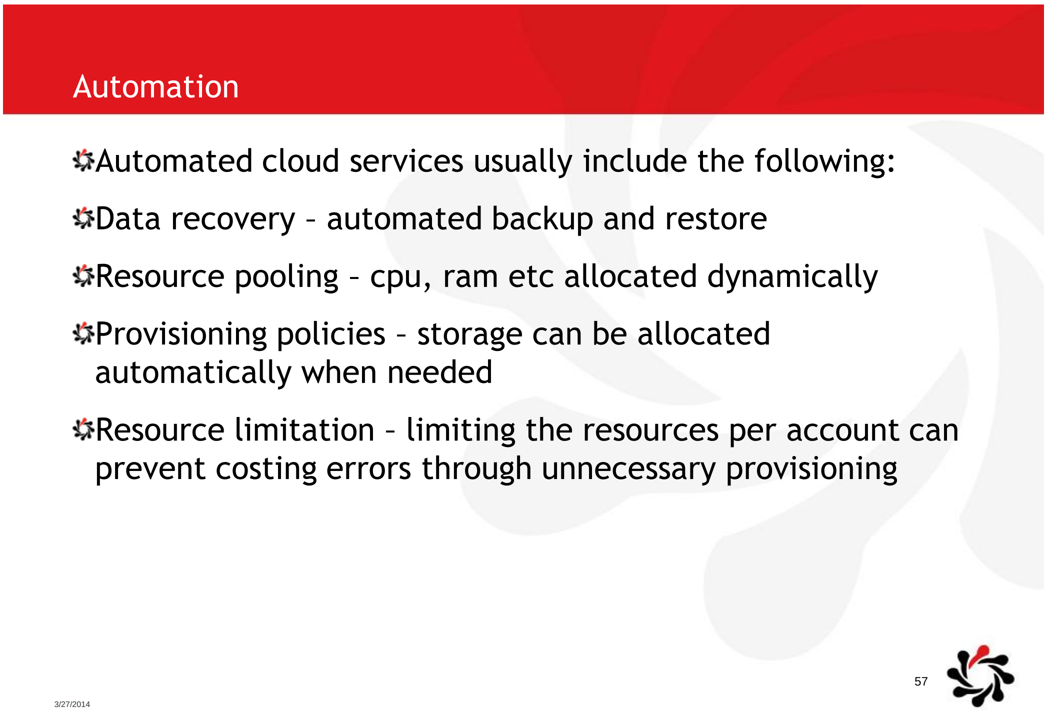
Number of network nodes – insufficient switches and routers

Hop count – how many nodes the data has to travel through

Protocol latency – high throughput requires high bandwidth

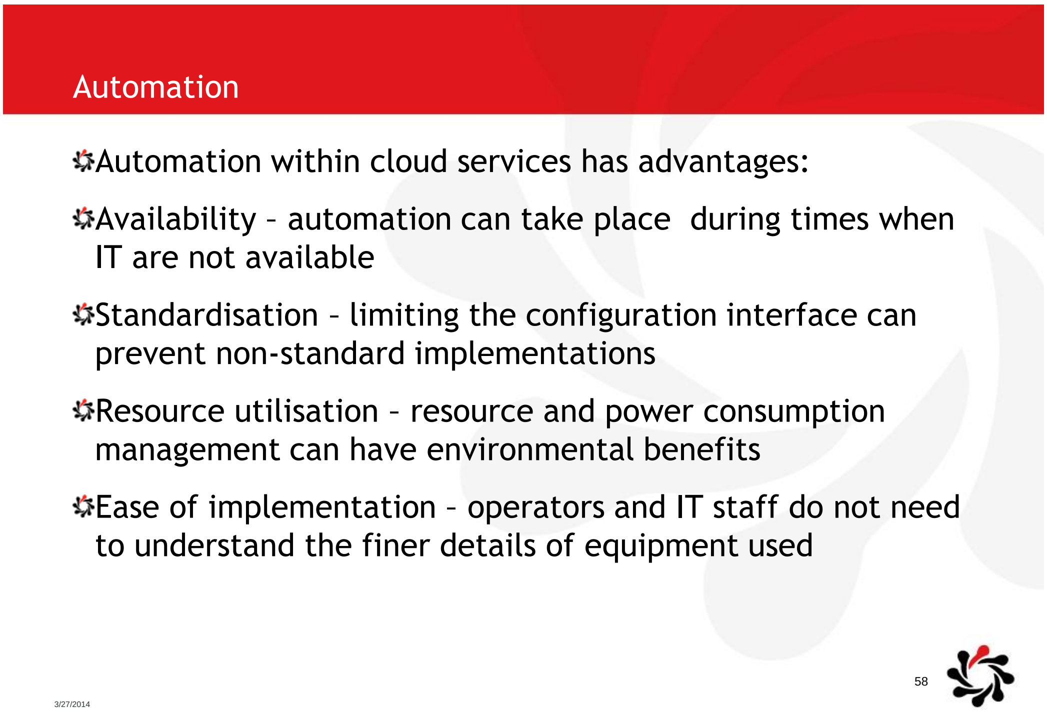
Automation

- A key element of cloud services is self-service provisioning which can be assisted through automation
- Management consoles allow IT staff to provision cloud resources
- Resources allocated to virtual servers can be increased or reduced



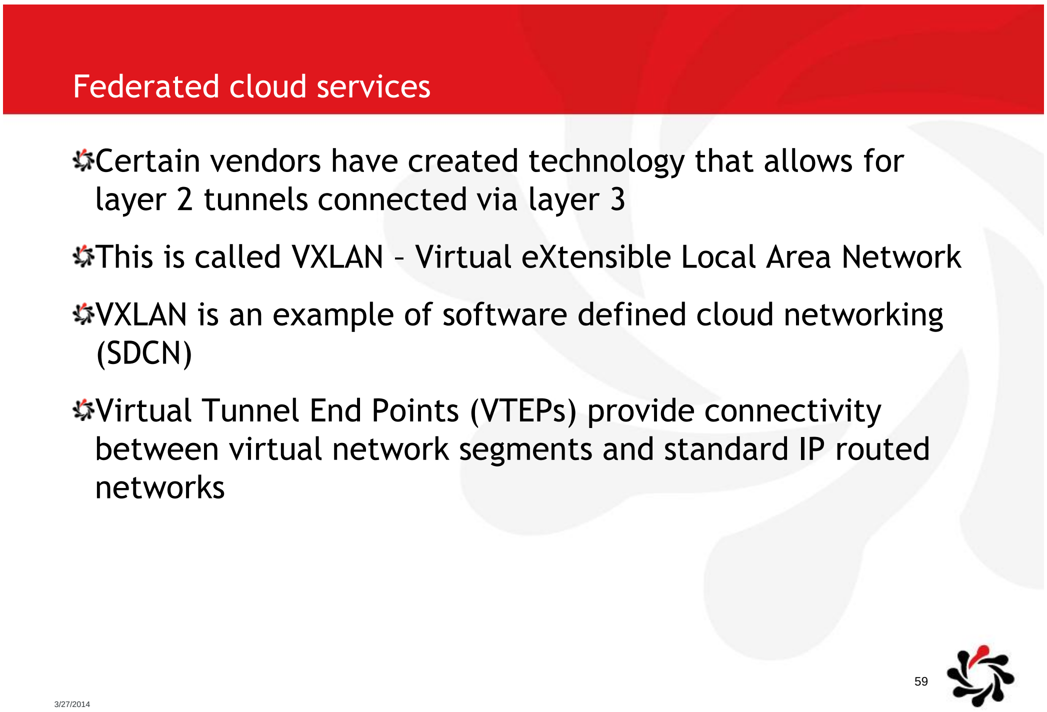
Automation

- Automated cloud services usually include the following:
- Data recovery – automated backup and restore
- Resource pooling – cpu, ram etc allocated dynamically
- Provisioning policies – storage can be allocated automatically when needed
- Resource limitation – limiting the resources per account can prevent costing errors through unnecessary provisioning



Automation

- Automation within cloud services has advantages:
- Availability – automation can take place during times when IT are not available
- Standardisation – limiting the configuration interface can prevent non-standard implementations
- Resource utilisation – resource and power consumption management can have environmental benefits
- Ease of implementation – operators and IT staff do not need to understand the finer details of equipment used

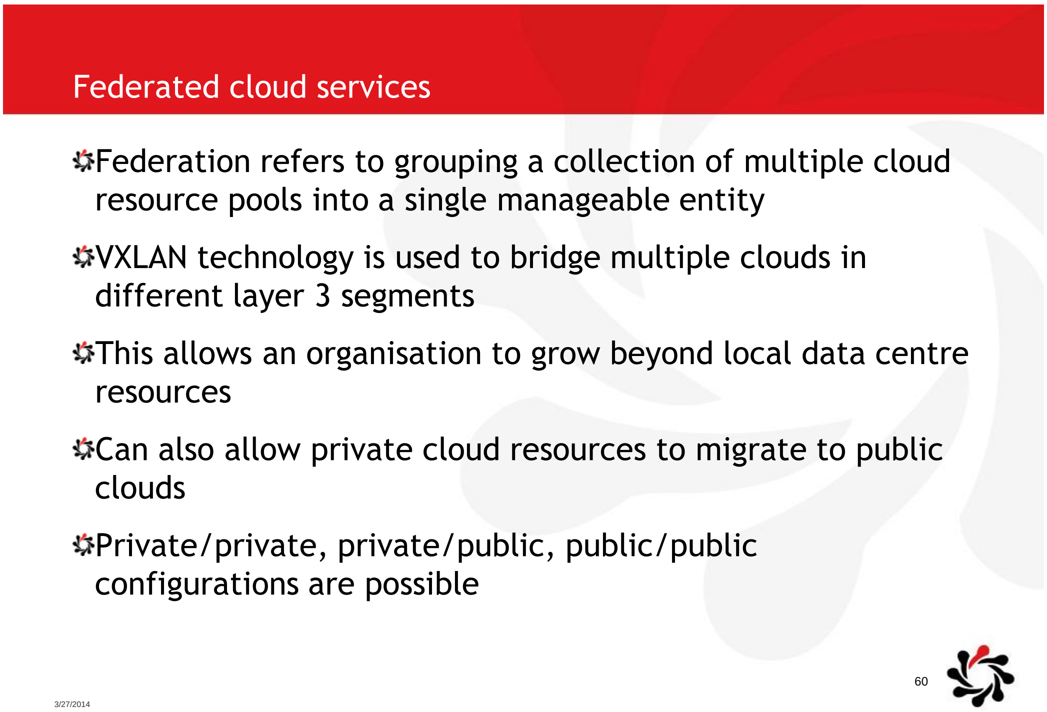


Federated cloud services

- Certain vendors have created technology that allows for layer 2 tunnels connected via layer 3
- This is called VXLAN – Virtual eXtensible Local Area Network
- VXLAN is an example of software defined cloud networking (SDCN)
- Virtual Tunnel End Points (VTEPs) provide connectivity between virtual network segments and standard IP routed networks

3/27/2014

59



Federated cloud services

- Federation refers to grouping a collection of multiple cloud resource pools into a single manageable entity
- VXLAN technology is used to bridge multiple clouds in different layer 3 segments
- This allows an organisation to grow beyond local data centre resources
- Can also allow private cloud resources to migrate to public clouds
- Private/private, private/public, public/public configurations are possible

3/27/2014

60

Federated cloud services

- Federated resources can be protected through encryption and digital certificates
- A storage gateway can be set up to provide pass through for cloud services supporting the following:

Backup and data recovery integration with other suites

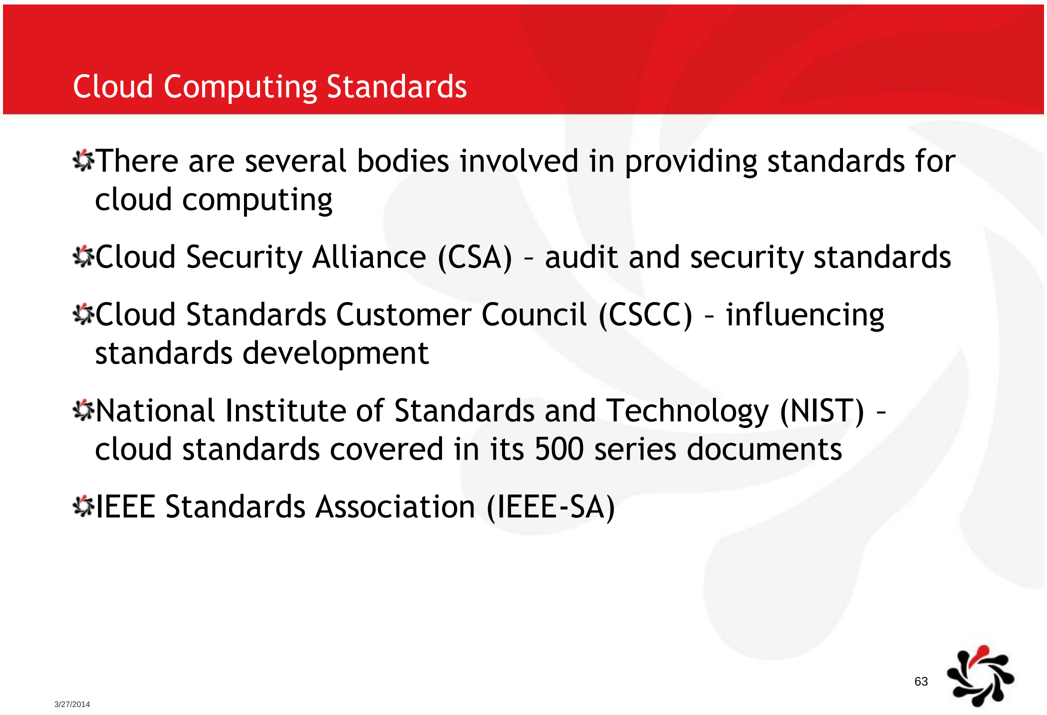
Caching to improve response times

Compression – reduce bandwidth requirements

Encryption – all data encrypted before transport and storage

Interoperability

- One of the biggest challenges is interoperability
- The ability to move resources between service providers
- The ability for services in different clouds to access common data
- Using common management tools across multiple providers
- Various vendors offer cloud orchestration tools



Cloud Computing Standards

- There are several bodies involved in providing standards for cloud computing
- Cloud Security Alliance (CSA) – audit and security standards
- Cloud Standards Customer Council (CSCC) – influencing standards development
- National Institute of Standards and Technology (NIST) – cloud standards covered in its 500 series documents
- IEEE Standards Association (IEEE-SA)

63

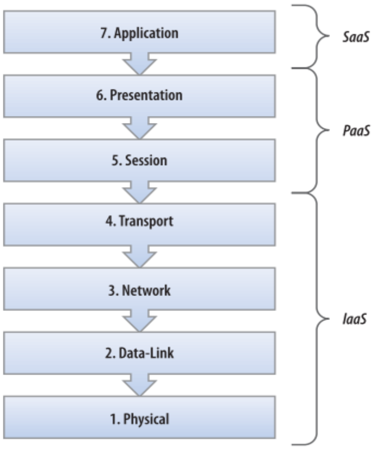
3/27/2014

Strategies for Cloud Adoption

64

3/27/2014

- Cloud services and their alignment with OSI


7. Application

6. Presentation

5. Session

4. Transport

3. Network

2. Data-Link

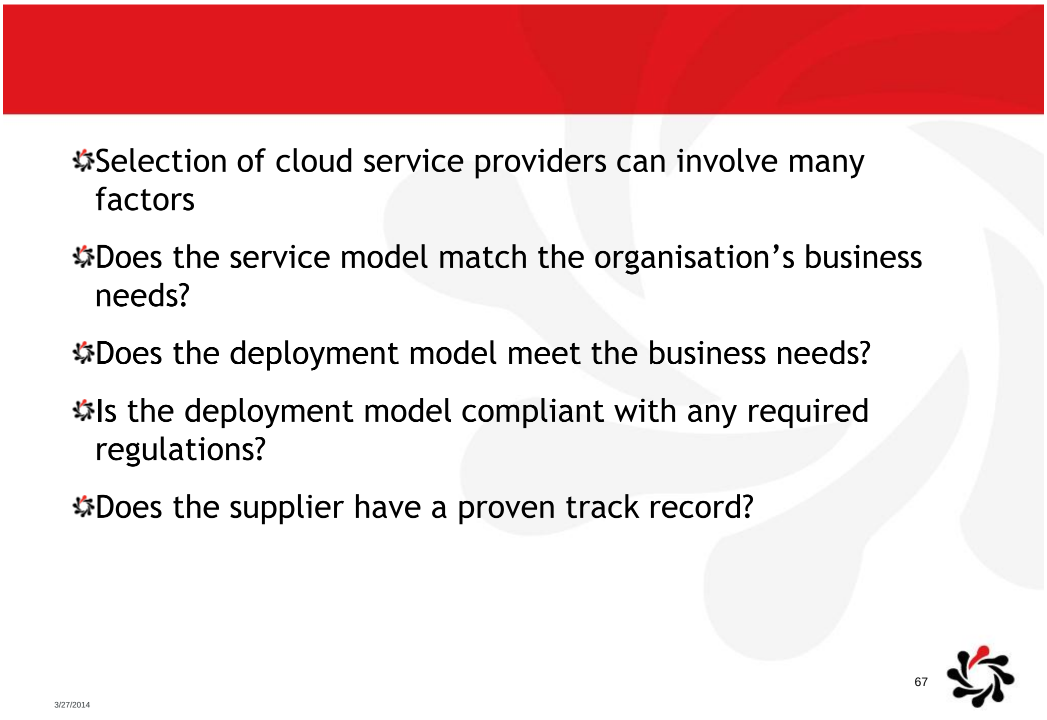
1. Physical

SaaS

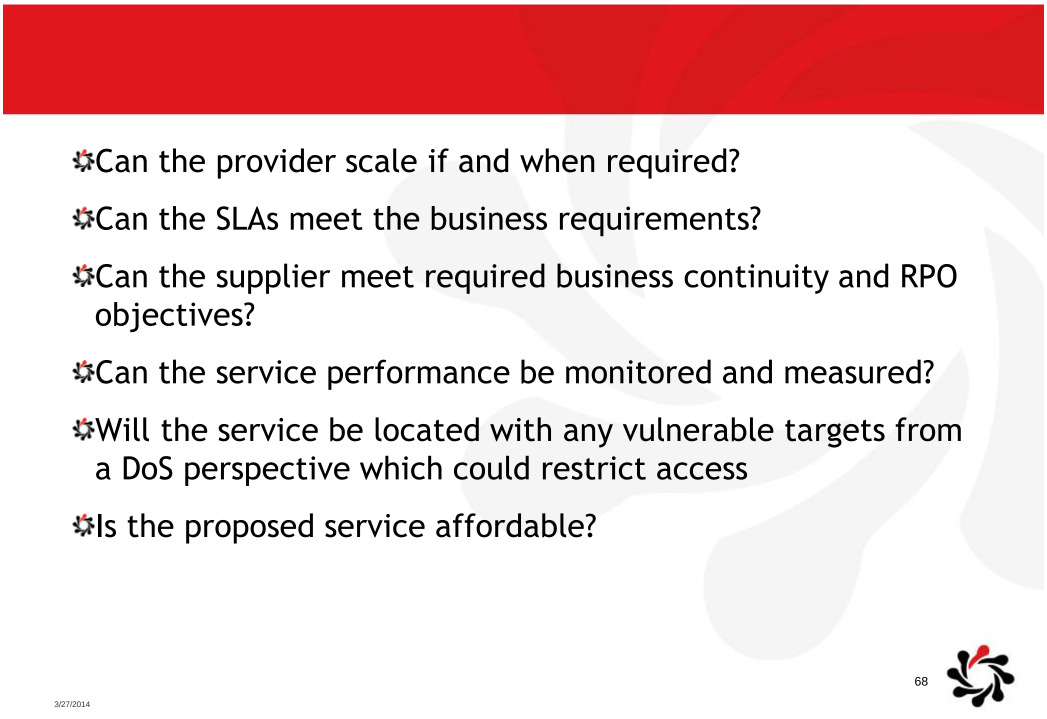
PaaS

IaaS

- Organisations need to understand the type of cloud service they will be using and how it maps to the networking architecture
- This assists in aligning prospective cloud deployments with organisational goals
- Different providers can provide one or more type of service



- Selection of cloud service providers can involve many factors
- Does the service model match the organisation’s business needs?
- Does the deployment model meet the business needs?
- Is the deployment model compliant with any required regulations?
- Does the supplier have a proven track record?

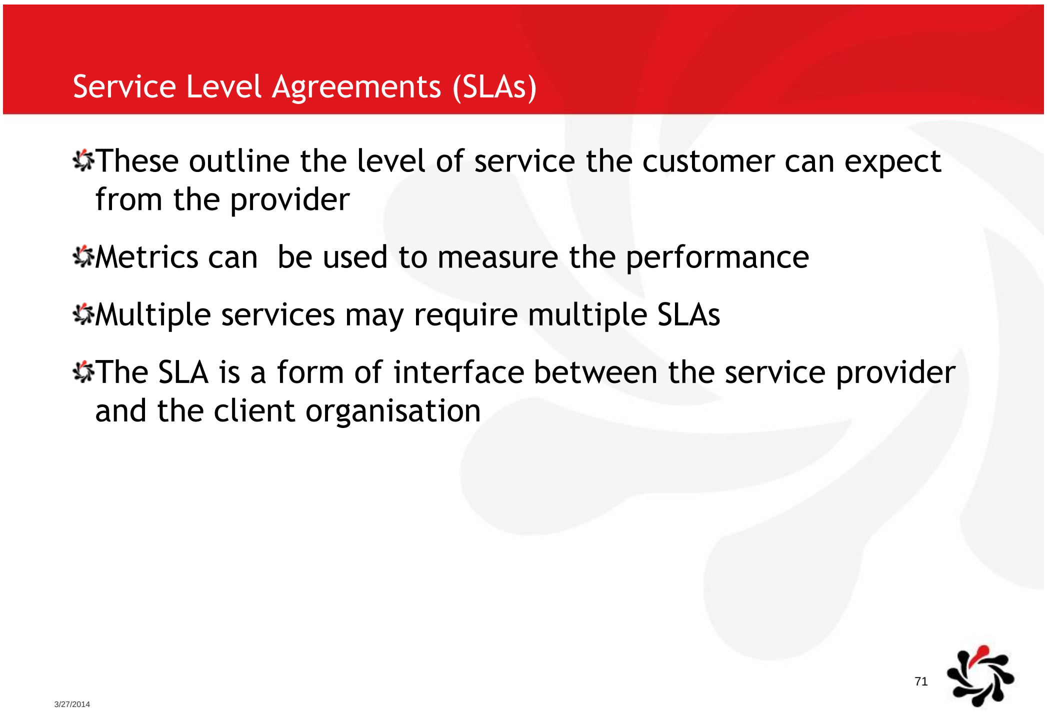


- Can the provider scale if and when required?
- Can the SLAs meet the business requirements?
- Can the supplier meet required business continuity and RPO objectives?
- Can the service performance be monitored and measured?
- Will the service be located with any vulnerable targets from a DoS perspective which could restrict access
- Is the proposed service affordable?

- What is the impact of adopting cloud services?
- Changing the culture of the business
- Change in financial processes from Capital to Operational
- Changes in the risk model – where is the data and how safe is it?
- Changes to infrastructure and service management

- Ready for the cloud?

1. Initiate a pilot to test viability
2. Cloud requirements should be based upon business needs
3. Ensure the plan is clearly communicated and understood
4. Review pilot results and address any issues

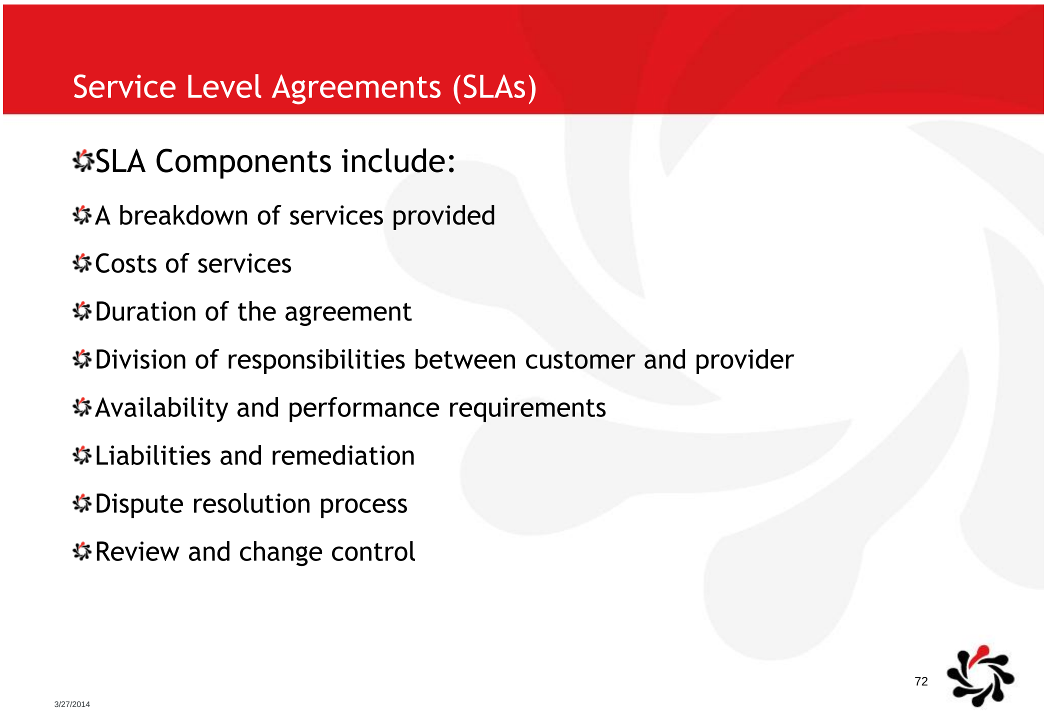


Service Level Agreements (SLAs)

- These outline the level of service the customer can expect from the provider
- Metrics can be used to measure the performance
- Multiple services may require multiple SLAs
- The SLA is a form of interface between the service provider and the client organisation

3/27/2014

71



Service Level Agreements (SLAs)

- SLA Components include:
- A breakdown of services provided
- Costs of services
- Duration of the agreement
- Division of responsibilities between customer and provider
- Availability and performance requirements
- Liabilities and remediation
- Dispute resolution process
- Review and change control

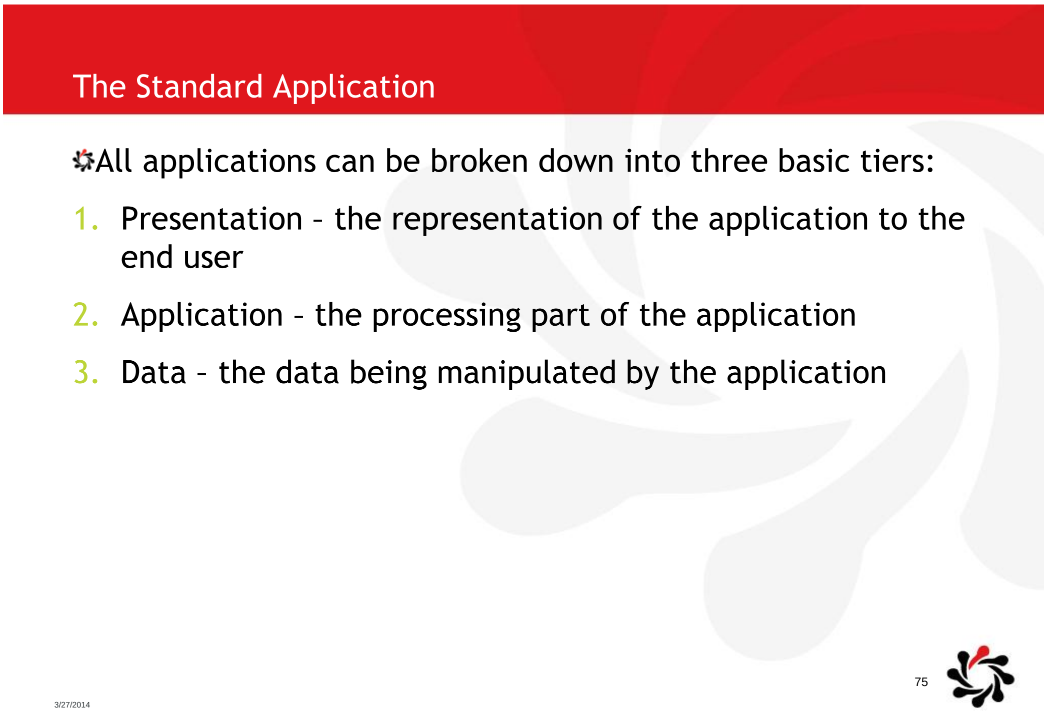
3/27/2014

72

Service Level Agreements (SLAs)

- Cloud services have their own specific considerations:
- Data location
- Service multitenancy
- Data breach considerations
- DR process notifications
- Data ownership

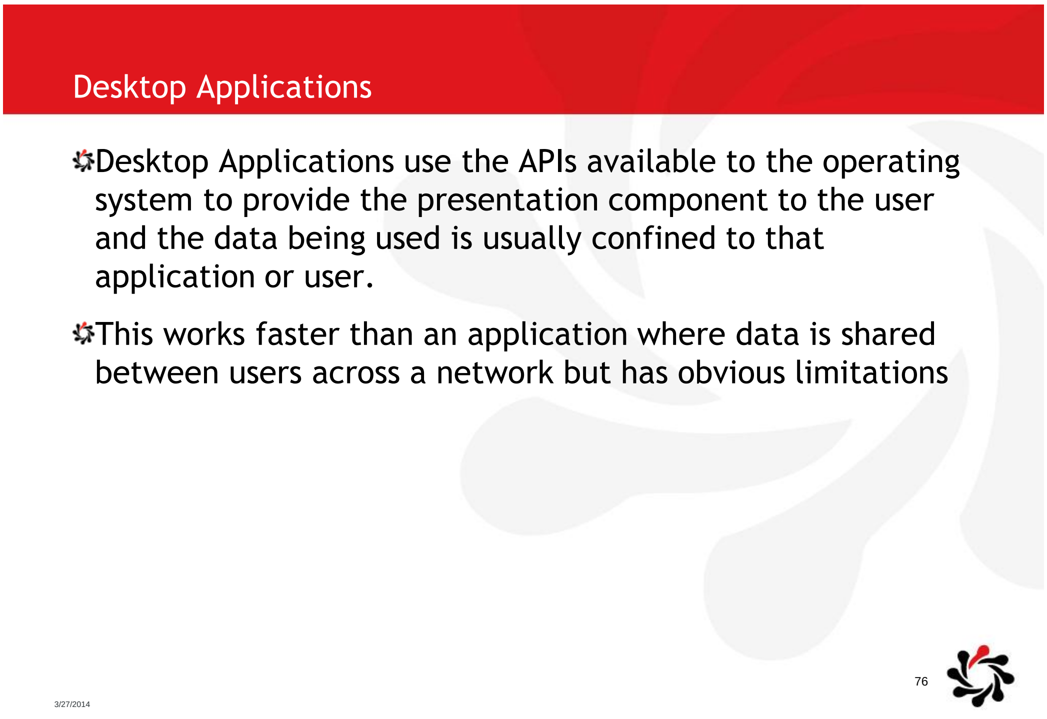
Applications in the Cloud



The Standard Application

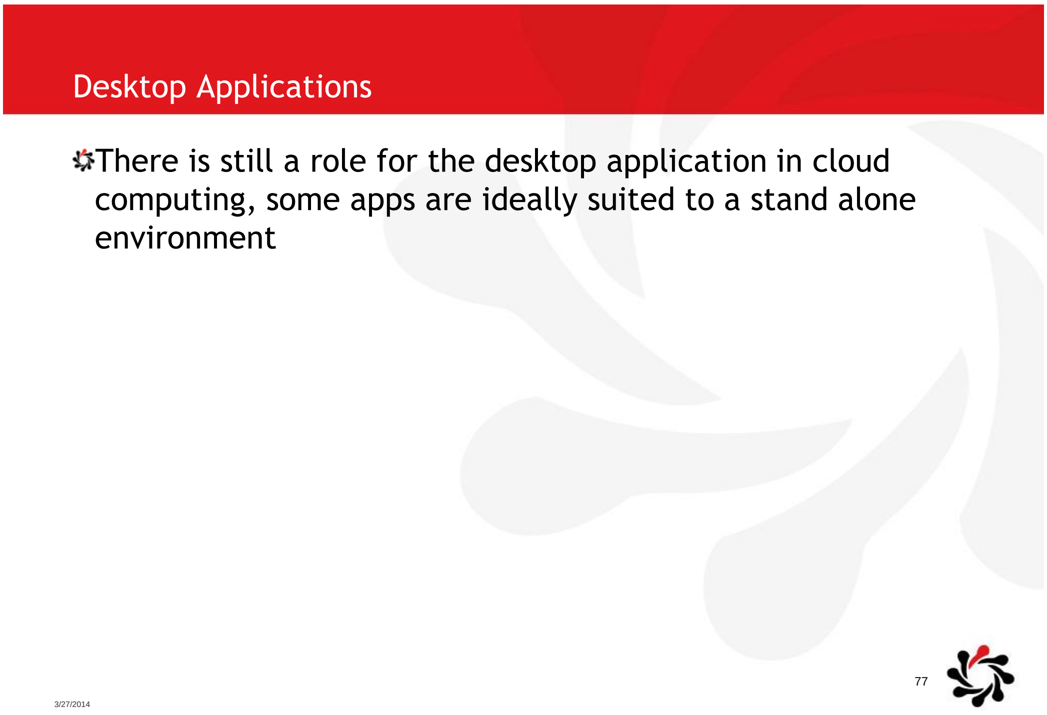
- All applications can be broken down into three basic tiers:

1. Presentation – the representation of the application to the end user
2. Application – the processing part of the application
3. Data – the data being manipulated by the application



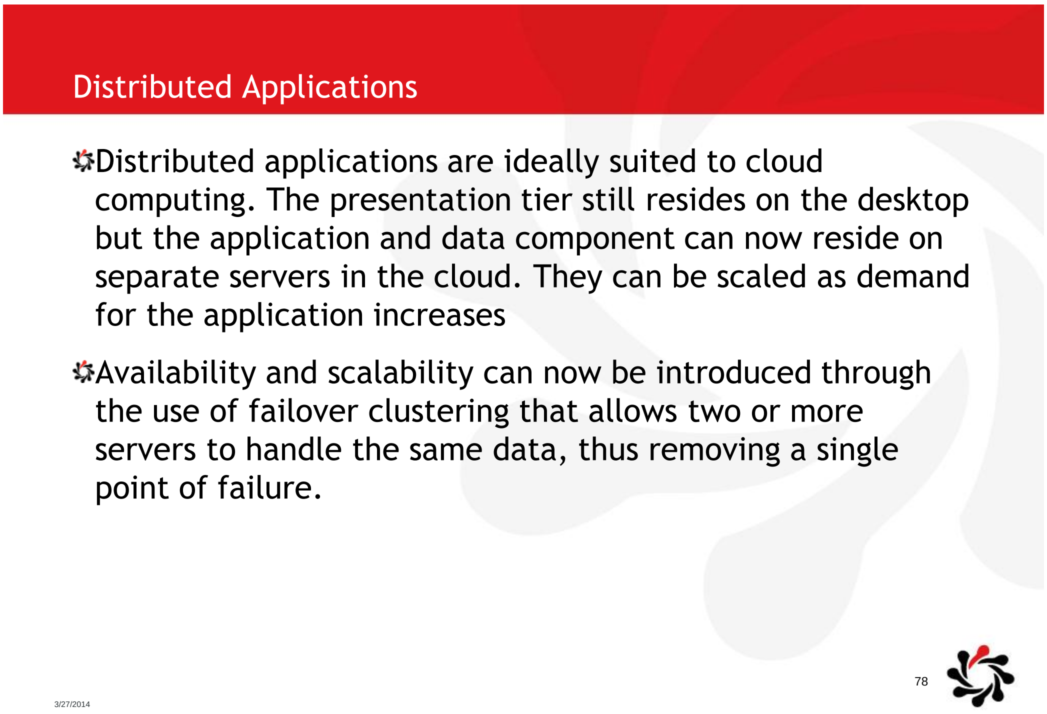
Desktop Applications

- Desktop Applications use the APIs available to the operating system to provide the presentation component to the user and the data being used is usually confined to that application or user.
- This works faster than an application where data is shared between users across a network but has obvious limitations



Desktop Applications

- There is still a role for the desktop application in cloud computing, some apps are ideally suited to a stand alone environment



Distributed Applications

- Distributed applications are ideally suited to cloud computing. The presentation tier still resides on the desktop but the application and data component can now reside on separate servers in the cloud. They can be scaled as demand for the application increases
- Availability and scalability can now be introduced through the use of failover clustering that allows two or more servers to handle the same data, thus removing a single point of failure.

Web Based Applications

- The web-based application allows for a more consistent interface working through a browser with the connection typically over the Internet.
- This now provides for portability and mobility because the application can now be accessed through a wider range of devices that are location independent

Cloud Applications

- The difference between Web and cloud applications is tenuous. The cloud application takes all the advantages of the web based app and extends it by providing additional scalability, resilience and security
- Costs are reduced from the web based model because we can now provision and on-demand model rather than a fixed web infrastructure that exists regardless of demand

Developing Cloud Applications

- Not all applications can migrate to the cloud.
- Potential cloud apps should be identified then modified so they are cloud ready
- Cloud ready means the application can scale out when demand warrants and scale down when demand decreases

Developing Cloud Applications

- Cloud applications should be developed around four main patterns of activity
- Start small, grow fast – a typical scenario for startup organisations. Publish the application and scale according to demand, no heavy investment going to waste if the product flops
- Predictable burst – burst of demand can be linked to single or particular events which are predicted and the application can be scaled around these for short periods

Developing Cloud Applications

- Unpredictable burst – unforeseen events can cause unexpected demand for service, difficult to plan for but scalability within the data centre can mitigate this

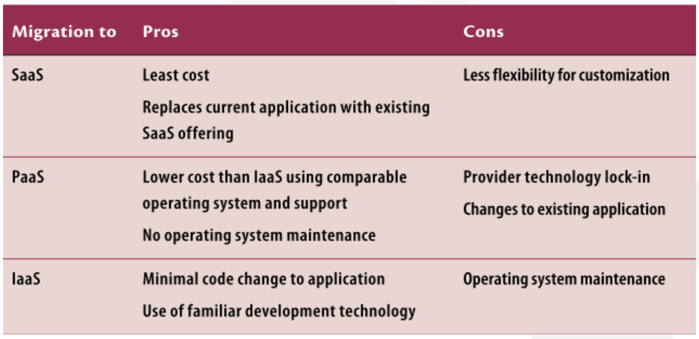
- Periodic processing – applications that are heavily used for certain periods of time then go through very slack periods. Monthly and annual processing tasks are examples of this. Using the cloud can avoid unnecessary investment in equipment that is only needed sporadically.

Developing Cloud Applications

- There are two main factors when developing cloud apps
- Stateful or stateless – stateful apps have to maintain information between calls to a server whereas in the cloud you cannot guarantee the same server responding to requests so stateless apps are preferred
- IaaS vs PaaS – different providers use different APIS based upon their platforms so this should be checked to avoid being locked into a particular API

Migrating Applications to the Cloud

- Several factors must be considered when migrating existing applications to the cloud. Some migrate easily, other have costs attached to them



Migration to	Pros	Cons
SaaS	Least cost Replaces current application with existing SaaS offering	Less flexibility for customization
PaaS	Lower cost than IaaS using comparable operating system and support No operating system maintenance	Provider technology lock-in Changes to existing application
IaaS	Minimal code change to application Use of familiar development technology	Operating system maintenance

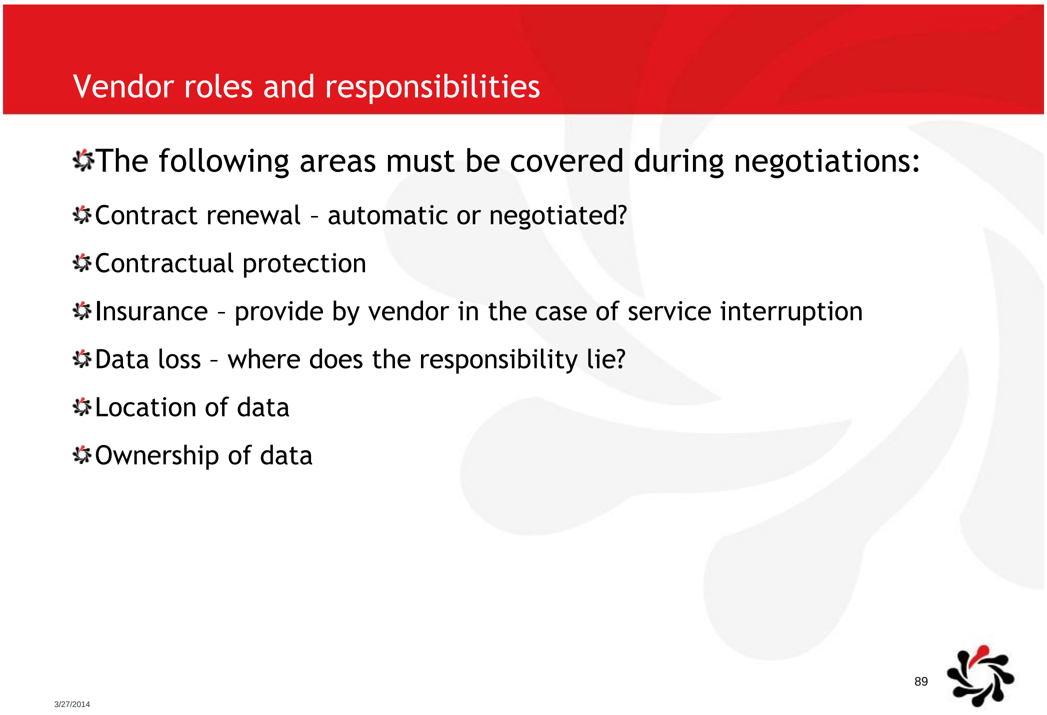
Technical Challenges

- Big data – applications that generate vast amount of data like log files can cost a lot of money
- Unstructured data – flat files can require greater computing resources that can ramp up costs
- Security – PII and other types of data require protection in the cloud
- Compliance – certain countries do not allow data to cross geographical boundaries
- Learning Curve – staff need to be trained in the development of cloud based applications

Cloud Service Rollout

Vendor roles and responsibilities

- Any service agreement must contain a list of roles and responsibilities for both customer and vendor
- Part of the decision making process as to which vendor is the ability to agree the legal terms of the agreement
- Terms must be present in the service agreement to guarantee service delivery and define the actions in the case of non-delivery

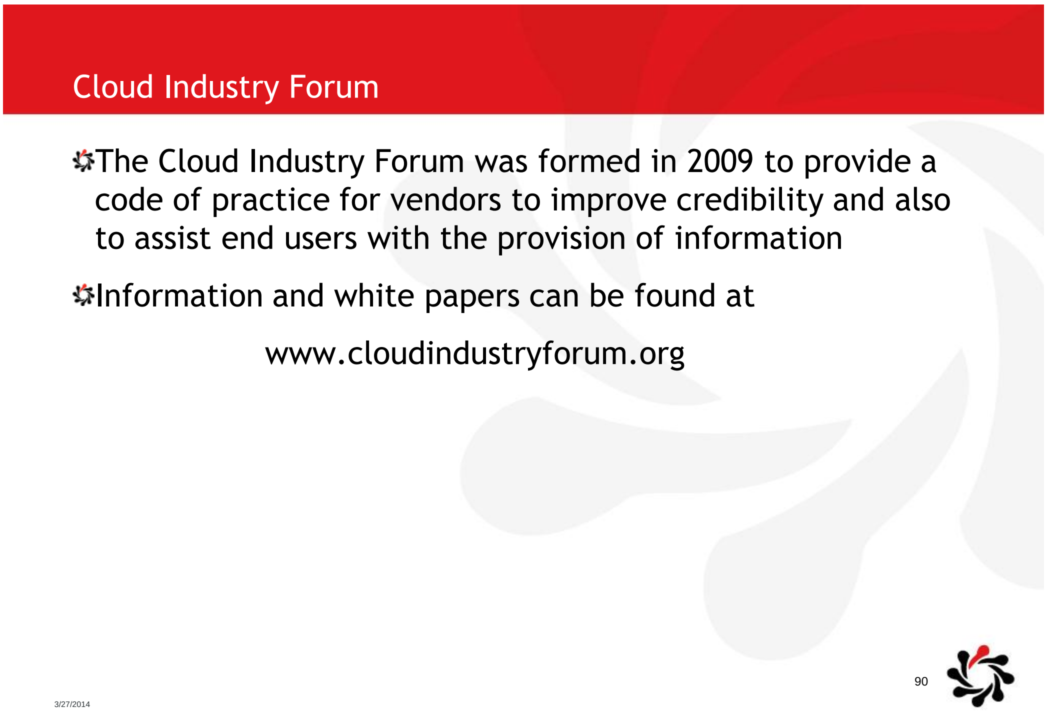


Vendor roles and responsibilities

- The following areas must be covered during negotiations:
- Contract renewal – automatic or negotiated?
- Contractual protection
- Insurance – provide by vendor in the case of service interruption
- Data loss – where does the responsibility lie?
- Location of data
- Ownership of data

3/27/2014

89



Cloud Industry Forum

- The Cloud Industry Forum was formed in 2009 to provide a code of practice for vendors to improve credibility and also to assist end users with the provision of information
- Information and white papers can be found at

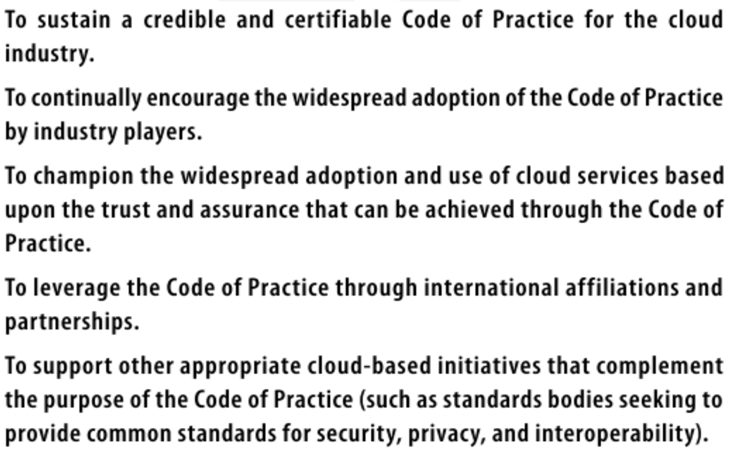
www.cloudindustryforum.org

3/27/2014

90

Cloud Industry Forum

- The goals of the Cloud Industry Forum are as follows:



To sustain a credible and certifiable Code of Practice for the cloud industry.

To continually encourage the widespread adoption of the Code of Practice by industry players.

To champion the widespread adoption and use of cloud services based upon the trust and assurance that can be achieved through the Code of Practice.

To leverage the Code of Practice through international affiliations and partnerships.

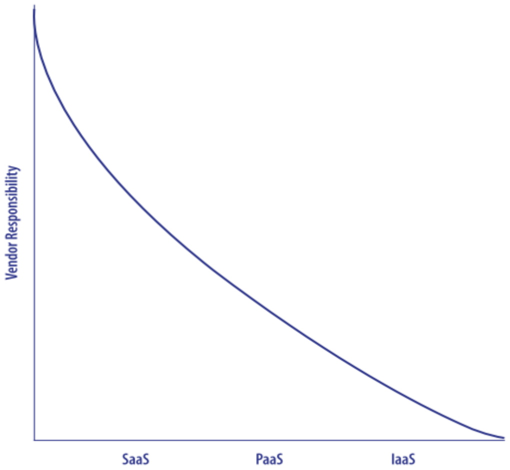
To support other appropriate cloud-based initiatives that complement the purpose of the Code of Practice (such as standards bodies seeking to provide common standards for security, privacy, and interoperability).

Best Practice

- Below are typical best practices for negotiating a cloud service contract
- Choice of law – this needs to consider territorial coverage
- Data control – where they are, backups etc
- Service availability
- Liabilities
- Deletion of data – customer must be notified if data is to be deleted

Vendor responsibilities

- These vary dependant upon the type of cloud service being provided



Organisational skill requirements

- The vendor has more technical responsibilities when transferring services to the cloud
- The customer still requires a level of knowledge to understand how the cloud functions and any limitations
- More than just technical skills are required to ensure that cloud services are being used in the best way for the organisation

Software as a Service

- Remember – SaaS is where the vendor provides access to the application
- The vendor maintains the application so organisational technical skills are minimum
- Help desk services could be provided by either party
- Monitoring tools should be available
- There may be a need to migrate local application data into the SaaS solution

Software as a Service

- New skills required:
- Project management
- Vendor management
- Business and financial skills
- Compliance knowledge
- Integration and analysis skills

Platform as a Service

- This time the vendor provides access to APIs and the infrastructure for virtual machines
- Skills required now include:
- Development skills for the API
- Project management skills
- Monitoring and migration skills as before
- Basic solution skills for help desk and training purposes

Infrastructure as a Service

- Vendors provide the hardware and connectivity necessary to maintain applications hosted on virtual machines
- The organisation technical skills include those required for other models plus the skills necessary for operating system deployment and maintenance, i.e. patch management
- Project management skills

Going live

- Transitioning from test to live environments will vary depending upon the type of cloud service being used
- SaaS is fairly transparent because no changes are required by the customer
- PaaS vendors typically provide test environments with VMs prior to going live. Migration tools may be provided
- IaaS is similar to PaaS but the availability of any migration tools should be checked

Going Live

- Other factors to take into account include:
- Internet Bandwidth – if local apps are now accessed over the Internet is there enough bandwidth available
- Network devices may need configuring to prioritise network traffic using services such as WAAS from Cisco
- WAN links – changes may have to be made with the anticipated increase in network traffic

Incident Management

- Each cloud vendor may have its own processes for incident management and utilise different tracking systems
- Is there a need for interoperability between vendor and end user incident management systems
- Some organisations may not have visibility of vendor incident management systems
- Using multiple vendors can lead to greater transparency issues

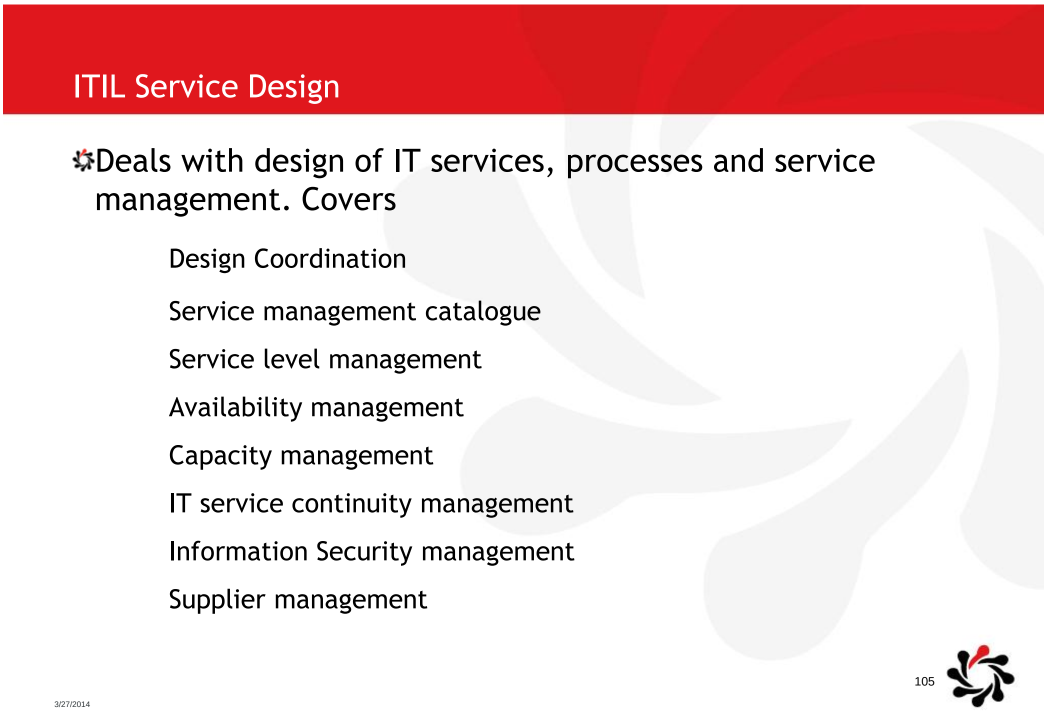
Cloud Service-Level Management

ITIL

- Information Technology Infrastructure Library (ITIL) is a framework of best practice processes that can be adopted to fit an organisation's environment
- A body of knowledge fitted into five volumes
  - Service Strategy
  - Service Design
  - Service Transition
  - Service Operation
  - Continual Process Improvement

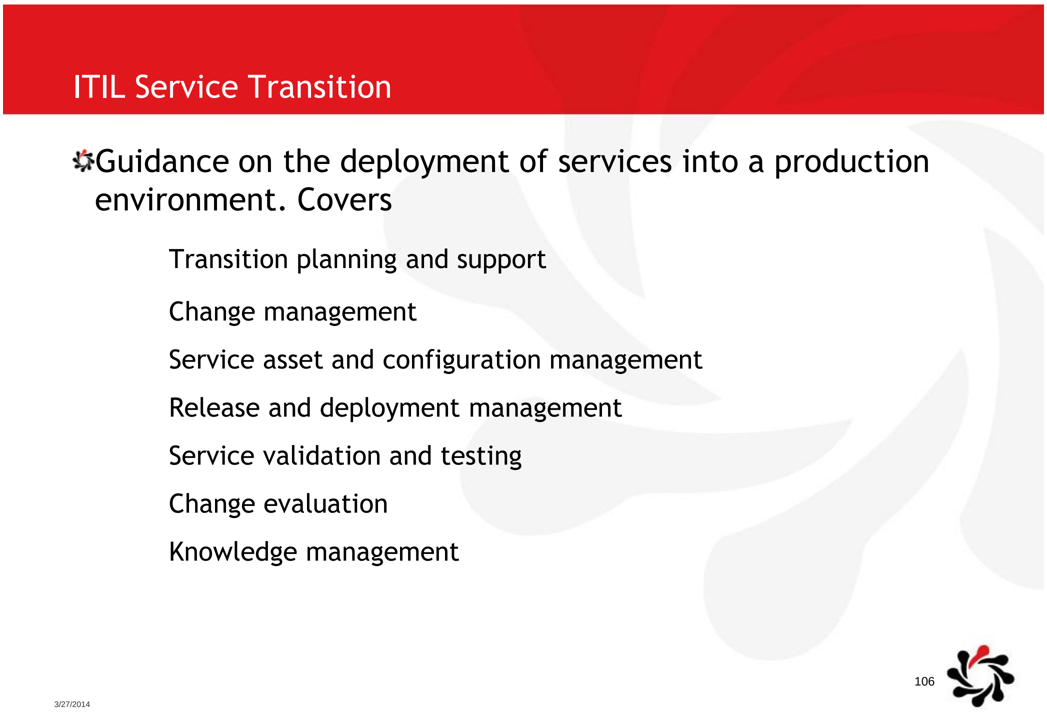
ITIL Service Strategy

- Deals with service provider investments in services
- Processes covered:
  - Strategy Management
  - Demand Management
  - Service Portfolio Management
  - Financial Management
  - Business Relationship Management



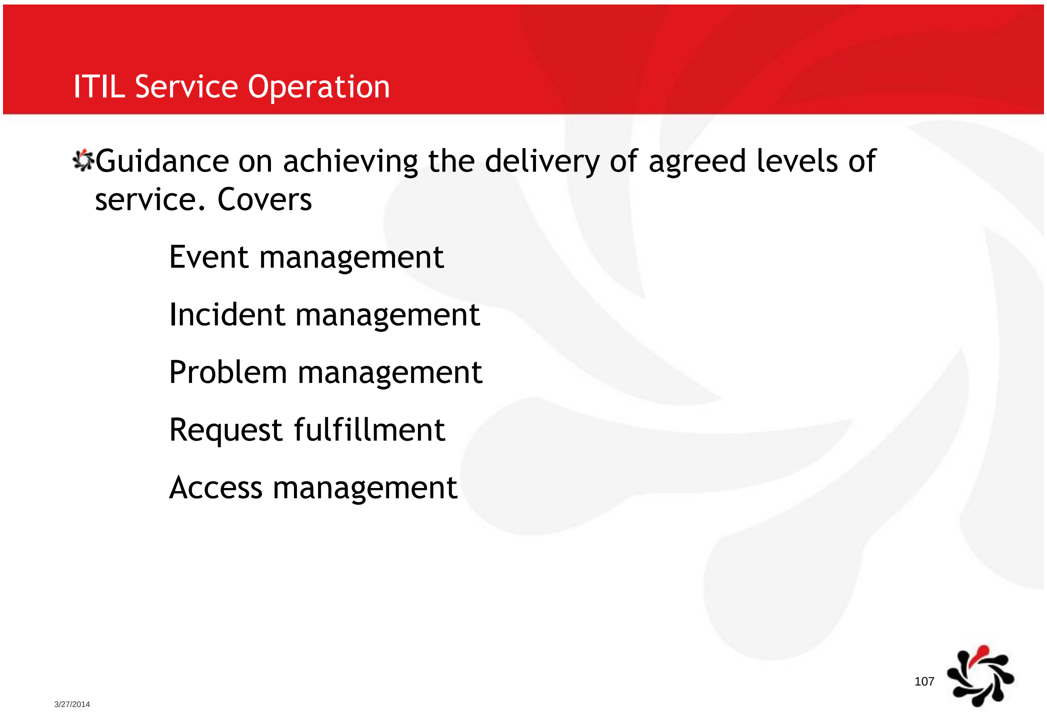
ITIL Service Design

- Deals with design of IT services, processes and service management. Covers
    - Design Coordination
    - Service management catalogue
    - Service level management
    - Availability management
    - Capacity management
    - IT service continuity management
    - Information Security management
    - Supplier management



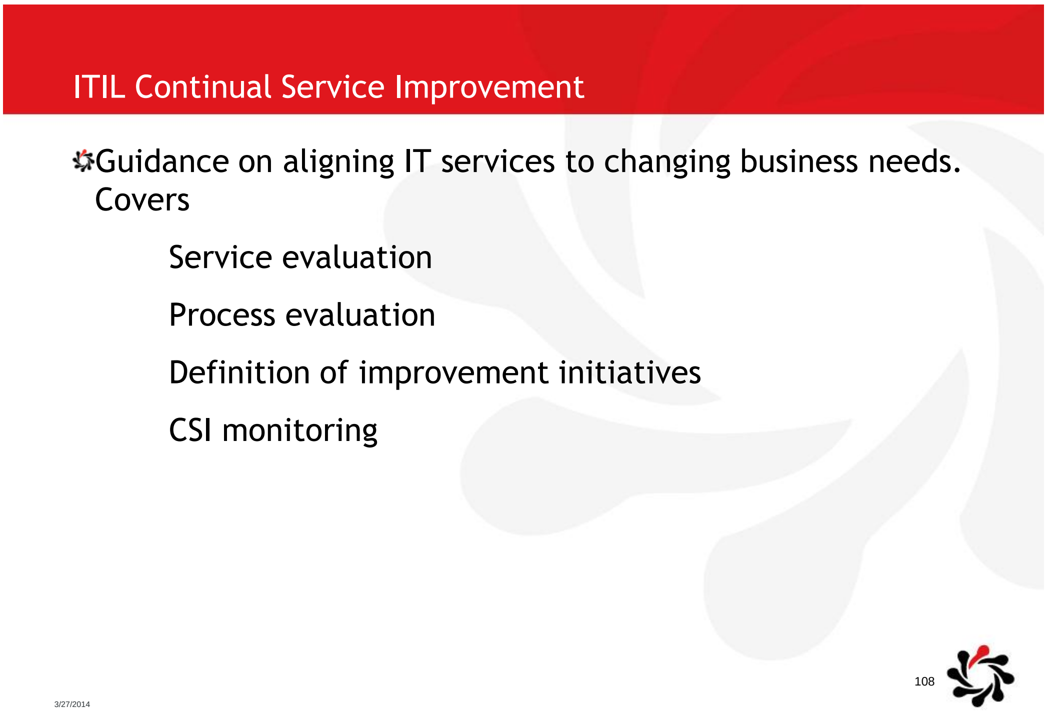
ITIL Service Transition

- Guidance on the deployment of services into a production environment. Covers
    - Transition planning and support
    - Change management
    - Service asset and configuration management
    - Release and deployment management
    - Service validation and testing
    - Change evaluation
    - Knowledge management



ITIL Service Operation

- Guidance on achieving the delivery of agreed levels of service. Covers
    - Event management
    - Incident management
    - Problem management
    - Request fulfillment
    - Access management



ITIL Continual Service Improvement

- Guidance on aligning IT services to changing business needs. Covers
    - Service evaluation
    - Process evaluation
    - Definition of improvement initiatives
    - CSI monitoring

Service Portfolio Management

- An organisation may have a range of applications and cloud based services
- A well defined portfolio management process keeps track of existing services and relates events and monitoring to each service in the CMDB (Configuration Management Database)
- The CMDB is a centralised database that contains information about the entire enterprise architecture:

  services, hardware, settings, users and processes

- Financial Management

  Processes should be in place to manage service costs

  This can be used to produce ROI information
- Business Relationship Management

Processes that are out in place to manage the relationship between the IT organisation and the customer

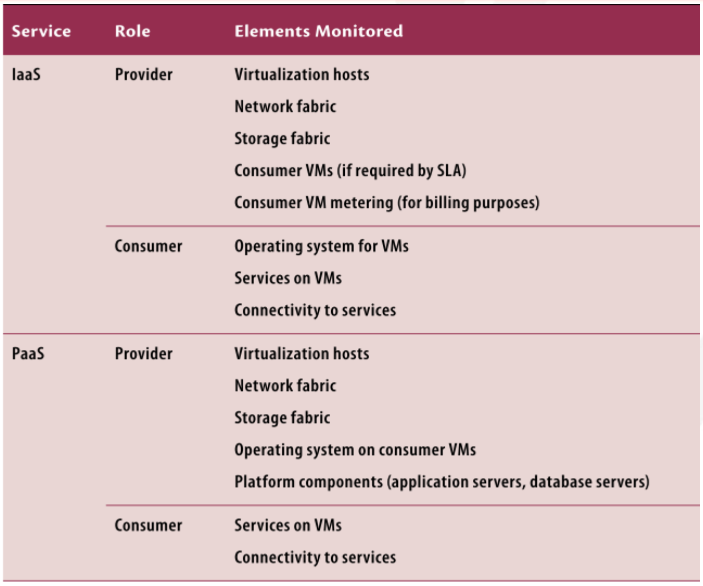
Service Desk

- The service desk is the single point of contact to provide the communication between users and the IT organisation
- When using cloud services you must define how to handle request and incidents for these services. With SaaS the vendor handles incidents but you may only want to run one service desk and use that as the conduit to the vendor service desk

Performance Metrics

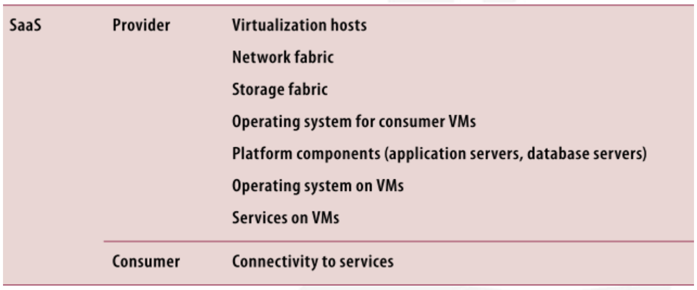
- When using cloud services you need to understand how to monitor those services and what performance metrics to look for
- The metrics used depend upon the type of cloud service being used

Performance Metrics



Service	Role	Elements Monitored
IaaS	Provider	Virtualization hosts Network fabric Storage fabric Consumer VMs (if required by SLA) Consumer VM metering (for billing purposes)
	Consumer	Operating system for VMs Services on VMs Connectivity to services
PaaS	Provider	Virtualization hosts Network fabric Storage fabric Operating system on consumer VMs Platform components (application servers, database servers)
	Consumer	Services on VMs Connectivity to services

Performance Metrics



SaaS	Provider	Virtualization hosts Network fabric Storage fabric Operating system for consumer VMs Platform components (application servers, database servers) Operating system on VMs Services on VMs
	Consumer	Connectivity to services

Security in the cloud

- The principle aims of information security are Confidentiality, Integrity, and Availability

- Confidentiality – the sensitivity of data, protected from unauthorised access, use or disclosure
- Integrity – the reliability of the data, protected from unauthorised modification
- Availability – accessibility of the data, protected from disruption of service

Security Controls

- Security controls can protect the CIA triad
- Controls can minimise the effect of security incidents
- Security controls can be Management, Technical, or Operational

Security Controls

- Management Controls – include the standards, policies and guidelines to provide the overall framework
- Technical Controls – these are applied to the IT resources. Can include access controls, firewall rules, encryption etc. Can also include physical security controls to prevent unauthorised physical access
- Operational Controls – processes and procedures carried out by individuals, includes DR planning and incident response

Security Controls

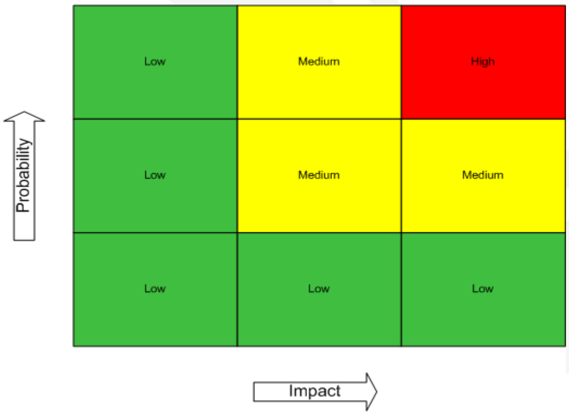
- Defence in depth – a layered approach to security starting with perimeter defences like firewalls and ending with host protection but including policies, procedures, network security etc.

Risk Management

- A brief overview of the risk management process
- Identify the assets – this can now include virtual assets and who the owners are
- Identify threats and vulnerabilities – every threat has an associated vulnerability. These range from natural disasters, through human error, to hackers

Risk Management

- Assess risk – evaluate the likelihood of each threat being exploited and determine the impact. Assign values to the risk and then a simple matrix can be used



Low	Medium	High
Low	Medium	Medium
Low	Low	Low

Risk Management

- Address risk – address in order of priority. Mitigate risk where possible. Risk can be transferred to third parties. There will always be an element of accepting risk. Risk cannot be ignored
- Monitor risk – perform monitoring to ensure that mitigation or other measures are effective

Security Standards

- Sets of rules, principles etc, that provide an approved model.
- There are many recognised standards and you should check that the cloud supplier follows standards
- Some of the better known security standards include:
  - COBIT 5 for Information Security from ISACA
  - ISO 27000 series
  - NIST series 800
  - Open Security Architecture (OSA)
  - Payment Card Industry (PCI-DSS)

Security Standards

- NIST has three publications specific to cloud computing:

1. SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing
2. SP800-145 The NIST Definition of Cloud Computing
3. SP800-146 Cloud Computing Synopsis and Recommendations

Common Security Risks

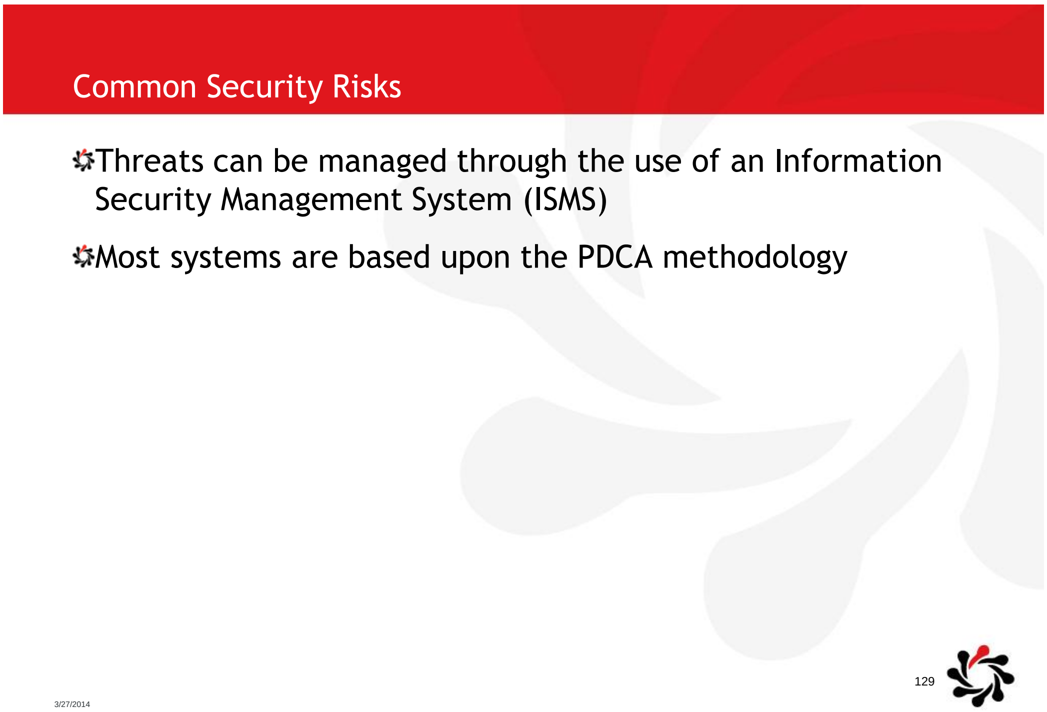
- Firewalls, when used in cloud environments need to be able to scale to customer needs. Likely to have redundant network and power connections to provide high availability
- Virtual firewalls exist in virtualised environments where they can protect virtual hosts
- VPNs are used to provide users with secure connections to cloud resources. When implementing VPNs check for compatibility issues

Common Security Risks

- Application Interface – needs to be hardened with secure programming practices to avoid exposing data and account information
- Shared resources – multitenancy agreements can lead to security risks. An attack against another customer could have an adverse effect on performance
- Insider threats – Cloud providers are not immune from inside threats and these can produce the highest risks to any organisation. Standard practice such as least privilege can mitigate this

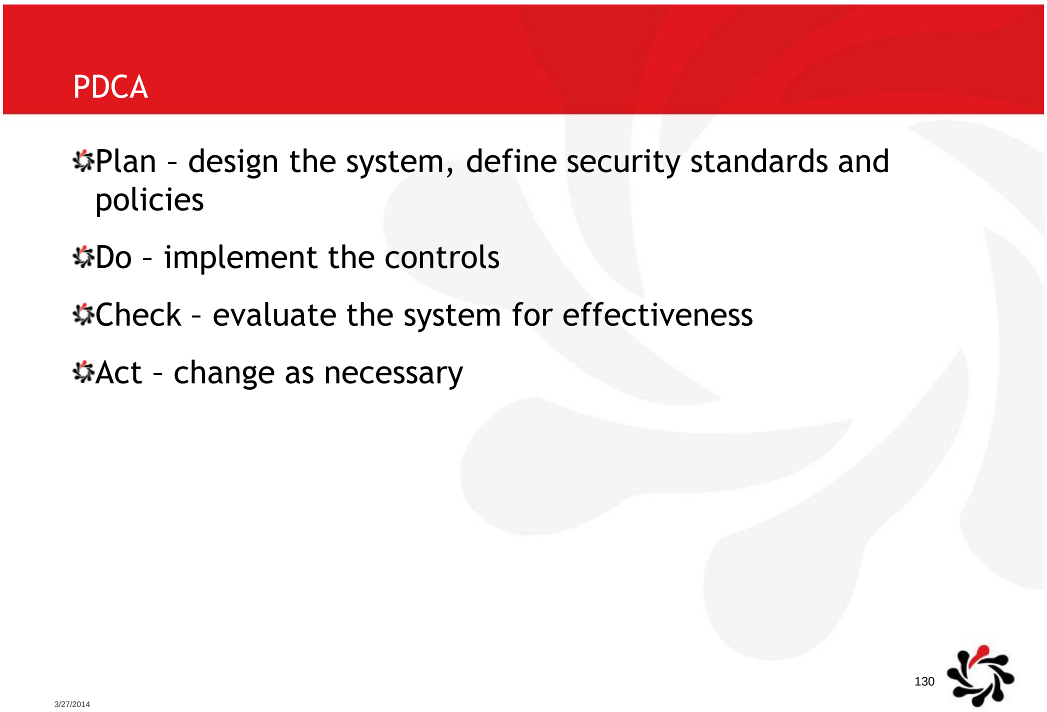
Common Security Risks

- Data exposure and loss – weak authentication and access controls can lead to exposure of data. Data loss can occur through accidental deletion or a security incident. Encryption is probably the best mitigation tool here.
- Organisational risks – the organisation could be exposed due to the loss of control. This could lead to improper risk management due to unknown risk exposure as a result of lack of transparency



Common Security Risks

- Threats can be managed through the use of an Information Security Management System (ISMS)
- Most systems are based upon the PDCA methodology



PDCA

- Plan – design the system, define security standards and policies
- Do – implement the controls
- Check – evaluate the system for effectiveness
- Act – change as necessary

Incident Response

- Incidents will occur. These can be interruptions of service, disasters, theft of equipment etc.
- Incident management – the process of planning for and responding to incidents, sometimes called incident response
- Incident response team – a group of employees trained to deal with incidents

Incident Response

- The cloud service provider and customer must have a clear understanding of the following:

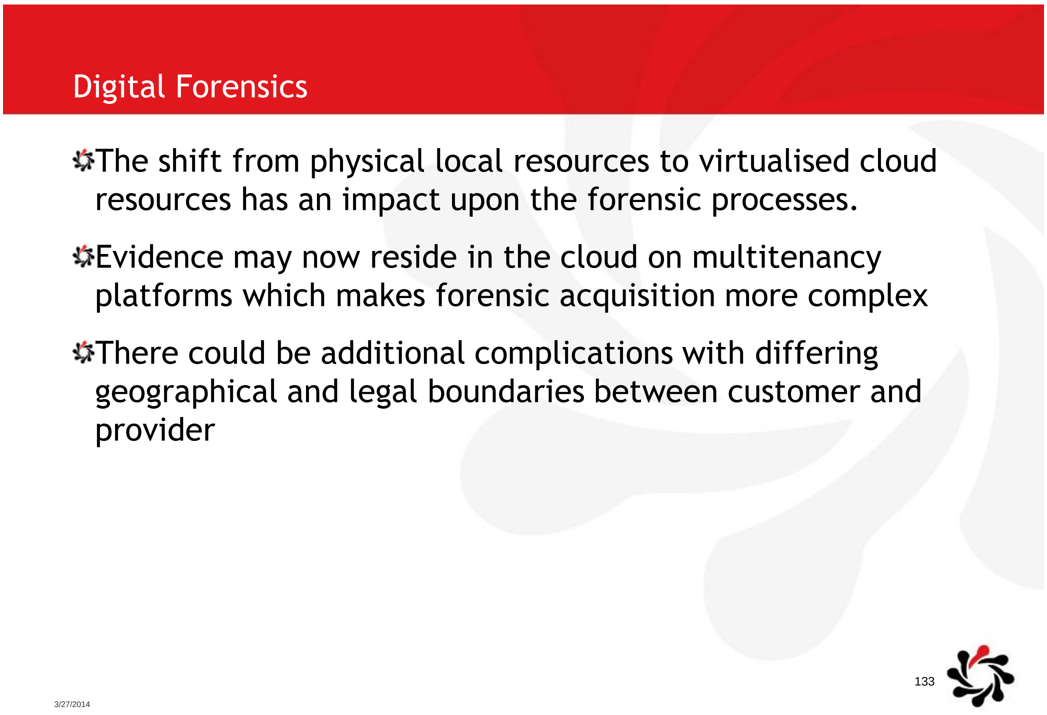
What is defined as an incident

The cloud provider’s responsibilities

Communications between customer and provider

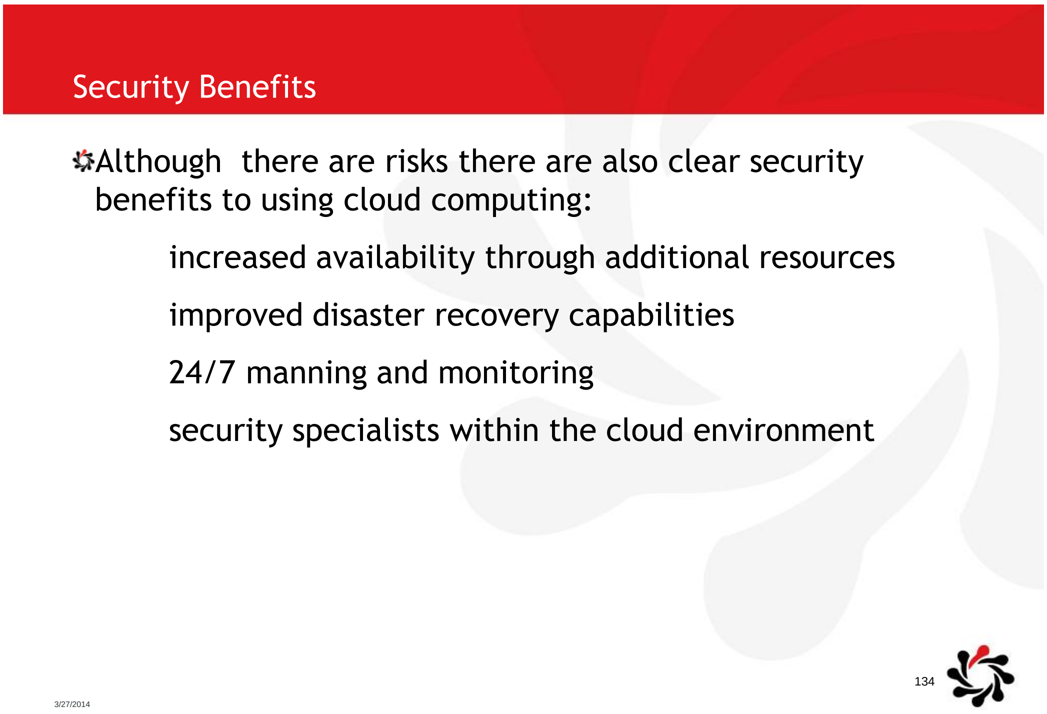
Recovery capabilities

Legal issues with data ownership



Digital Forensics

- The shift from physical local resources to virtualised cloud resources has an impact upon the forensic processes.
- Evidence may now reside in the cloud on multitenancy platforms which makes forensic acquisition more complex
- There could be additional complications with differing geographical and legal boundaries between customer and provider



Security Benefits

- Although there are risks there are also clear security benefits to using cloud computing:

increased availability through additional resources

improved disaster recovery capabilities

24/7 manning and monitoring

security specialists within the cloud environment

Privacy and Compliance

Legal Risks

- The ultimate legal responsibility and liability lies with the organisation or individual owning the data.
- The provider may have some responsibility as a custodian
- Data may be stored and processed in multiple locations in the cloud, anywhere in the world. This provide benefits for resiliency but can cause legal concerns

Legal Risks

- Data may be subject export restrictions and data in the cloud could be subject to laws based upon respective locations:

  Location of the physical servers

  Location of the provider’s headquarters

  ` ` Location of the data owner

  Locations the data passed through

The provider may be contractually required to keep data in certain locations

Legal Risks

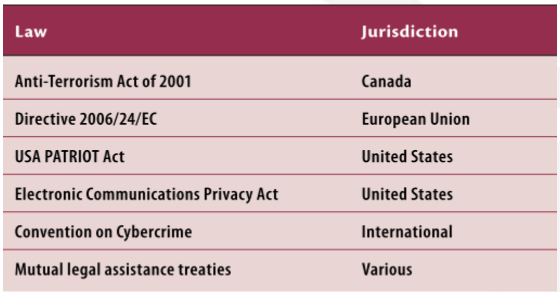
- Data isolation may be required for data security, i.e. physical separation. Can this be guaranteed in a multitenancy environment
- Data may also need to be isolated within a database
- Data deletion – what happens to the data when the contract comes to an end, assurances of secure deletion must be obtained
- Bankruptcy – what happens if the cloud provider goes out of business. Data may be exposed when assets are disposed of

Legal Risks

- Certain categories of data have specific legal requirements
- In the IS health records are covered by HIPAA (Health Insurance Portability Accountability Act)
- Professions such as Doctors and Lawyers have a requirement to keep client information confidential
- PII (Personally Identifiable Information) protection requirements will vary between jurisdictions

Legal Risks

- Lawful access and disclosure – government agencies may compel disclosure from service providers instead of from the data owner
- A summary of these regulations are shown below



Law	Jurisdiction
Anti-Terrorism Act of 2001	Canada
Directive 2006/24/EC	European Union
USA PATRIOT Act	United States
Electronic Communications Privacy Act	United States
Convention on Cybercrime	International
Mutual legal assistance treaties	Various

Compliance

- Software licensing in a traditional environment can be challenging, in the cloud it can be more so
- Traditional software licensing consists of Per User, Per Device, and Enterprise. These can all be interpreted in different ways when virtual environments are in use.
- Some existing licenses may not transfer into the cloud

Compliance

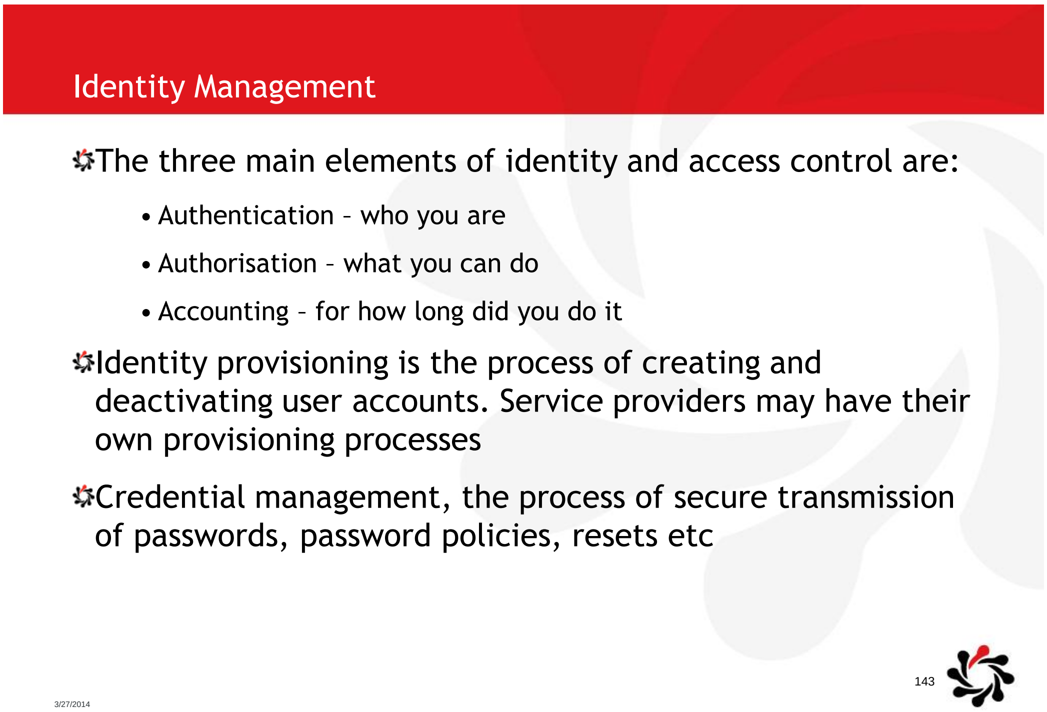
- Where possible, use a vendor that has a clear software licensing policy that can support:

Concurrency – based upon the number of users

Mobility – move between virtual environments

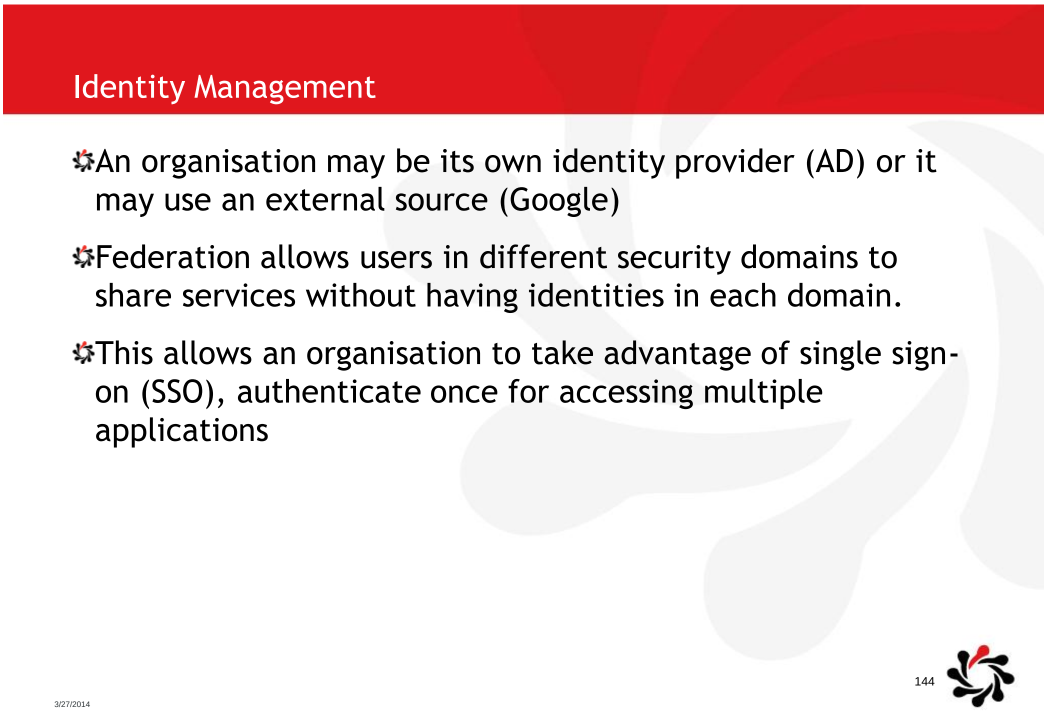
Flexibility – subscription or pay-as-you-go based upon need

Auto-scaling – cover for servers increasing or decreasing dynamically



Identity Management

- The three main elements of identity and access control are:
  - Authentication – who you are
  - Authorisation – what you can do
  - Accounting – for how long did you do it
- Identity provisioning is the process of creating and deactivating user accounts. Service providers may have their own provisioning processes
- Credential management, the process of secure transmission of passwords, password policies, resets etc



Identity Management

- An organisation may be its own identity provider (AD) or it may use an external source (Google)
- Federation allows users in different security domains to share services without having identities in each domain.
- This allows an organisation to take advantage of single sign-on (SSO), authenticate once for accessing multiple applications