Cloud Computing

What if your company or department only paid for the computing resources that it uses?

Then your company would not have to invest up front, as capital expenditure (CapEx), in purchasing the computing but simply sign up with a service provider on a **pay-as-you-use** billing model. This means that your company changes from a capital expenditure (CapEx) model to an operating expenditure (OpEx) one for meeting its computing needs

Remember: ***Cloud Computing*** – which promotes availability – is universal / convenient / on-demand access, via the internet, to computing resources – applications, servers (physical servers and virtual servers), data storage, development tools, and networking capabilities hosted at a remote data center managed by a cloud services provider (CSP)

Data Center

Remember: A data center is the facility that houses IT infrastructure of an organization (running / delivering applications and services, and storing / managing the data associated with those applications and services)

An optimal IT infrastructure:

- High-performance storage systems: store and back up data and include a data recovery system in case of disasters
- Low-inactivity networks: to reduce the delay of data flow
- Secure infrastructures: include systems that control information access and data availability. It can also safeguard a business against breaches and cyberattacks wherever the data resides, maintaining the customers' trust
- WANs: prioritize traffic and give certain applications more or less bandwidth as needed
- Zero downtime: reduce disruptions to business operations and eliminates system downtime to keep costs down and profits up

Data center infrastructure components:

- Rackmount / Blade Servers and /or Mainframes
- Storage Systems:
  - direct-attached storage (DAS) – enable the most frequently used data (hot data) to remain close the CPU
  - network-attached storage (NAS) – provides data storage and data access to multiple servers over a standard Ethernet connection. NAS is usually a dedicated server with multiple storage media—hard disk drives (HDDs) and/or solid-state drives (SSDs)
  - storage area network (SAN) – enables shared storage. SAN uses a separate network for the data and consists of a mix of multiple storage servers, application servers, and storage management software
- Networking: consisting of various types of switches, routers and fiber optics, carries network traffic across the servers (east/west traffic), and to / from the servers to the clients (north/south traffic)
- Power supply and cable Management: always-on
- Redundancy and disaster recovery
- Environmental controls: temperature, humidity, static electricity, fire

---

Virtualization

Remember: ***Virtualization*** uses software (Hypervisor, for example, VMware) to create an abstraction layer over computer hardware that allows the hardware elements of a single computer – processors, memory, storage etc. – to be divided into multiple virtual computers / machines (VMs). Each VM runs its own operating system (OS) and behaves like an independent computer, even though it is running on just a portion of the actual underlying computer hardware

Benefits of virtualization:

- Slash IT expenses: When virtualize an environment, a single physical server transforms into many virtual machines. These virtual machines can have different operating systems and run different applications while still all being hosted on the single physical server
- Reduce downtime and enhance resiliency in disaster recovery situations: With a virtualized environment, it's easy to provision and deploy, allowing to replicate or clone the virtual machine that's been affected. The recovery process would take minutes – as opposed to the hours it would take to provision and set up a new physical server
- Increase efficiency and productivity: Be able to install, update, and maintain the environment across all the VMs in the virtual environment on the server instead of going through the lengthy process of applying the updates server-by-server
- Control independence and DevOps: Developers can quickly spin up a virtual machine without impacting a production environment. It is ideal for Dev/Test, as the developer can quickly clone the virtual machine and run a test on the environment
- Move to be more green-friendly: Cut down on the number of physical servers used will lead to a reduction in the amount of power being consumed (Reduction in expenses and carbon footprint of a data center)

❖ Application Virtualization:

- delivers an application that is hosted on a single machine to a large number of users
- application can be situated in the cloud on high-grade virtual machines
- because a large number of users access it, its costs are shared by those users; makes the application cheaper to deliver to the end user
- end user does not need to have high-grade hardware in order to run the application
- if the data used by the virtual application are stored in the cloud, the user is not tethered to any one device or location to use the application or access its data (the virtual application is consumed through a mobile app or an Internet browser by the end user)

❖ Server Virtualization:

- uses common physical hardware (networks, storage, or computing machines) to host virtual machines
- physical host machine could have any number of virtual machines running on it so that one set of hardware is used to run different machines
- virtual machines can be installed with their own operating system and their own different set of applications

Traditional Architecture

Virtual Architecture

Enablers for Cloud Computing:

- Virtualization Technology
- Reporting
- Billing
- Demand Management
- Business Processes
- Tools

Cloud Computing Actors:

- Service Consumer
- Service Provider (provides cloud services to the cloud service consumer according to the Service Catalog)
- Service Creator (creates the service and supplies it to the service provider)
- Service Broker (acts as an intermediary between a service consumer and a number of service providers)

Characteristics of Cloud Computing:

- ubiquitous access (not constrained by where you are in order to use the cloud service)
- on-demand availability based on the consumer's self-service (consume the service whenever you want)
- pooling of resources
- rapid elasticity
- measured service usage

To Deploy a Cloud:

- standardize service offerings
- make service offerings available through simple portals
- track usage and cost information
- availability
- meet demand
- provide a security framework
- instantaneous reporting
- billing or charging mechanism on the basis of usage

Remember: In IT, a service is a collection of IT systems, components, and resources that work together to provide value to users

In order to measure and agree upon the value received, two parameters are usually used to assess a service:

- Cost
- Service Level Agreement (SLA); a contract between the service consumer and the service supplier in terms of how quickly the service will be delivered (when), its quality (what), and scope (where and how much)

  NOTE: Service Level Objectives (SLOs) are specific measurable characteristics of the SLA such as uptime, throughput, available resource capacity, response time, and delivery time

Service Models

❖ Software as a Service (SaaS)

SaaS, software-as-a-service, is application software hosted on the cloud and used over an internet connection via a web browser, mobile app or thin client

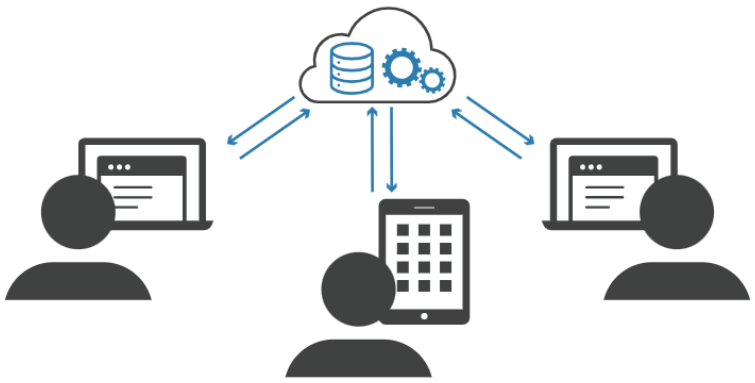
The SaaS provider is responsible for operating, managing and maintaining the software and the infrastructure on which it runs

The customer simply creates an account, pays a fee, and gets to work

The SaaS software vendor can host the application on its own cloud infrastructure or with a cloud service provider (such as Amazon Web Services (AWS), Google Cloud, IBM Cloud or Microsoft Azure)

The SaaS vendor is responsible for:

- Provisioning, managing and maintaining all the servers, networking equipment, storage hardware and operating software required to run the application
- Applying feature fixes and security patches as needed
- Providing load balancing, redundant infrastructure, data backup, cloud security and disaster recovery services to prevent outages and meet the performance, availability and data protection standards specified in the service level agreement (SLA)
- SaaS vendors may also provide an application programming interface (API) their customers can use to integrate the SaaS application with other SaaS or traditional software applications



Users can access SaaS applications on any device

SaaS advantages:

- SaaS removes the need for organizations to install and run applications on their own computers or in their own data centers. This eliminates the expense of hardware acquisition, provisioning, and maintenance, as well as software licensing, installation, and support

- Flexible Payments: Rather than purchasing software to install, or additional hardware to support it, customers subscribe to a SaaS offering. Transitioning costs to a recurring operating expense allows many businesses to exercise better and more predictable budgeting. Users can also terminate SaaS offerings at any time to stop those recurring costs

- Scalable Usage: Cloud services like SaaS offer high Vertical scalability, which gives customers the option to access more or fewer services or features on demand

- Automatic Updates: Rather than purchasing new software, customers can rely on a SaaS provider to automatically perform updates and patch management. This further reduces the burden on in-house IT staff

- Accessibility: Since SaaS vendors deliver applications over the internet, users can access them from any internet-enabled device and location

- Customization: SaaS applications are often customizable and can be integrated with other business applications, especially across applications from a common software provider

SaaS challenges and risks:

- Businesses must rely on outside vendors to provide the software, keep that software up and running, track and report accurate billing and facilitate a secure environment for the business's data

- Issues Beyond Customer Control: Issues can arise when providers experience service disruptions, impose unwanted changes to service offerings or experience a security breach – all of which can have a profound effect on the customers' ability to use the SaaS offering. To proactively mitigate these issues, customers should understand their SaaS provider's SLA and make sure it is enforced

- Customers Lose Control Over Versioning: If the provider adopts a new version of an application, it will roll out to all of its customers, regardless of whether or not the customer wants the newer version. This may require the organization to provide extra time and resources for training

- Difficulty Switching Vendors: To switch vendors, customers must migrate very large amounts of data. Furthermore, some vendors use proprietary technologies and data types, which can further complicate customer data transfer between different cloud providers. Vendor lock-in is when a customer cannot easily transition between service providers due to these conditions

- Security & Compliance: With SaaS applications, the responsibility for protecting those applications and their data moves from internal IT teams to the external SaaS providers. For small to medium-sized businesses, this is less of a disadvantage, as large cloud providers typically have more resources for putting strong security in place. But this can be a challenge if a large business faces tight security or regulatory standards. In some cases, businesses will be unable to assess their applications' security themselves, for instance by performing penetration testing

❖ Platform as a Service (PaaS)

PaaS, Platform-as-a-Service, is a cloud computing model that provides customers a complete cloud platform – hardware, software, and infrastructure – for developing, running, and managing applications without the cost, complexity, and inflexibility that often comes with building and maintaining that platform on-premises

The PaaS provider hosts everything – servers, networks, storage, operating system software, databases, development tools – at their data center

Customers can pay a fixed fee to provide a specified amount of resources for a specified number of users, or they can choose 'pay-as-you-go' pricing to pay only for the resources they use

PaaS advantages:

- Faster Time to Market: PaaS is used to build applications more quickly than would be possible if developers had to worry about building, configuring, and provisioning their own platforms and backend infrastructure. With PaaS, all they need to do is write the code and test the application, and the vendor handles the rest

- One Environment from Start to Finish: PaaS permits developers to build, test, debug, deploy, host, and update their applications all in the same environment. This enables developers to be sure a web application will function properly as hosted before they release, and it simplifies the application development lifecycle

- Price: PaaS is cost-effective. PaaS customers don't need to manage and provision virtual machines. In addition, some providers have a pay-as-you-go pricing structure, in which the vendor only charges for the computing resources used by the application, usually saving customers money. However, each vendor has a slightly different pricing structure, and some platform providers charge a flat fee per month

- Ease of Licensing: PaaS providers handle all licensing for operating systems, development tools, and everything else included in their platform

PaaS challenges and risks:

- Vendor Lock-in: It may become hard to switch PaaS providers, since the application is built using the vendor's tools and specifically for their platform. Each vendor may have different architecture requirements. Different vendors may not support the same languages, libraries, APIs, architecture, or operating system used to build and run the application. To switch vendors, developers may need to either rebuild or heavily alter their application

- Vendor Dependency: The effort and resources involved in changing PaaS vendors may make companies more dependent on their current vendor. A small change in the vendor's internal processes or infrastructure could have a huge impact on the performance of an application designed to run efficiently on the old configuration. Additionally, if the vendor changes their pricing model, an application may suddenly become more expensive to operate

- Security & Compliance Challenges: The PaaS vendor will store most or all of an application's data, along with hosting its code. In some cases, the vendor may actually store the databases via a further third party.

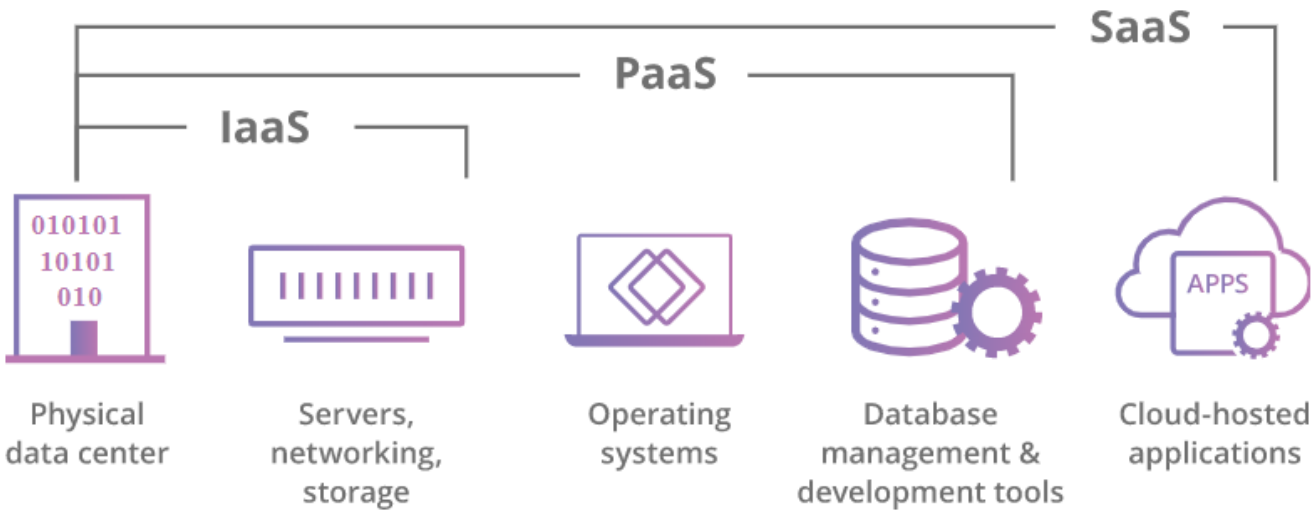
  Though most PaaS vendors are large companies with strong security in place, this makes it difficult to fully assess and test the security measures protecting the application and its data. In addition, for companies that have to comply with strict data security regulations, verifying the compliance of additional external vendors will add more hurdles to going to market

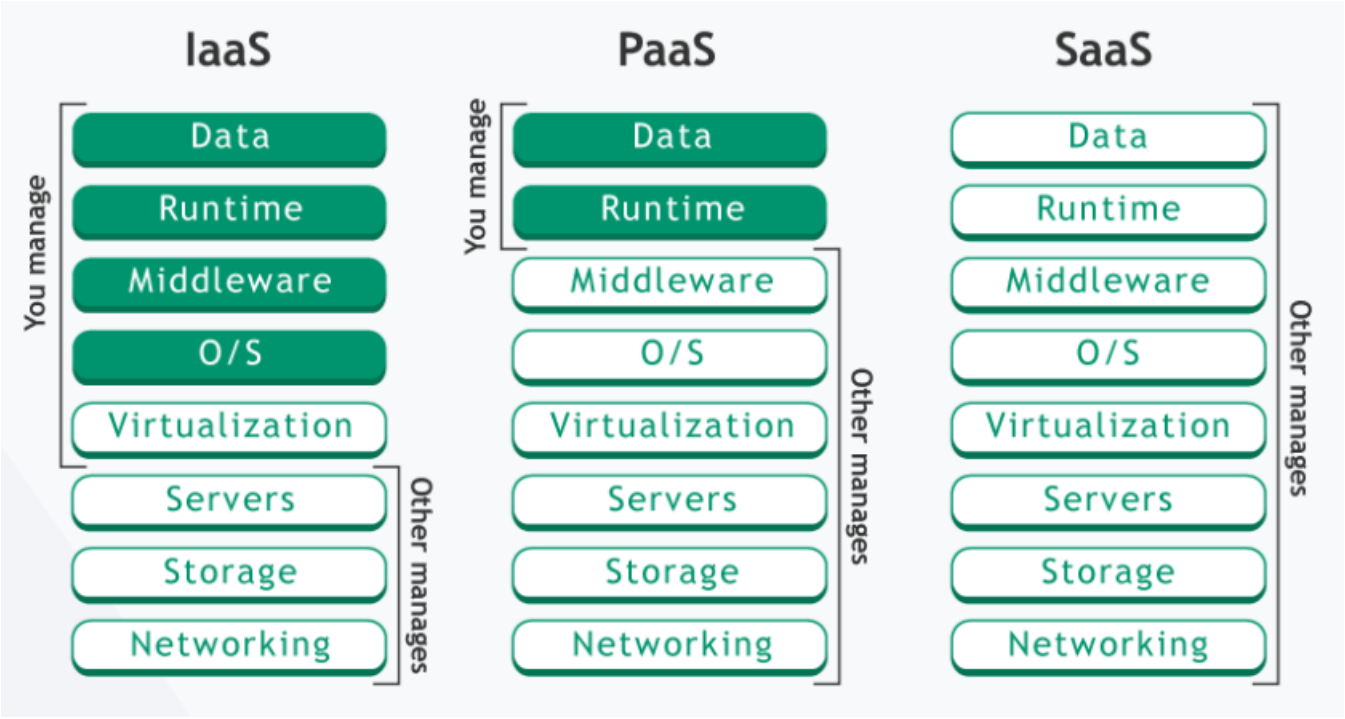
❖ Infrastructure as a Service (IaaS)

IaaS, Infrastructure-as-a-Service, is a form of cloud computing that delivers fundamental compute, network, and storage resources to consumers on-demand, over the internet, and on a pay-as-you-go basis

IaaS enables end users to scale and shrink resources on an as-needed basis, reducing the need for high, up-front capital expenditures or unnecessary “owned” infrastructure

The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)


SaaS
PaaS
IaaS
010101
10101
010
APPS
Physical data center
Servers, networking, storage
Operating systems
Database management & development tools
Cloud-hosted applications


IaaS
PaaS
SaaS
You manage
Other manages
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking

❖ Business Process as a Service (BPaaS)

The capability provided to the consumer is to replace a business function by a cloud service. BPaaS combines business process outsourcing (BPO) – companies outsource non-core activities – with cloud computing technology to provide a flexible way to implement IT-intensive business processes

Information Technology:

- Software development
- IT support
- Network management
- Data center operations

Knowledge Process:

- Research and development
- Data analysis
- Market research

Legal Process:

- Contract management
- Document review
- Legal research

Human Resources:

- Recruitment
- Payroll processing
- Employee benefits
- Training

Finance & Accounting:

- Accounts payable and receivable
- Financial reporting
- Tax preparation

BPaaS advantages:

- Cost reduction: Third-party service providers can offer their services at a lower cost due to their specialized expertise, resulting in lower operational costs
- Improved efficiency: Staff will focus on important tasks instead of the non-core functions
- Access to specialized expertise: Third-party service providers often have a team of experts with the necessary skills and experience to handle complex business processes
- Scalability: Scale operations up or down quickly without having to invest in additional resources or infrastructure

BPaaS challenges:

- Quality control: Organizations need to establish effective quality control measures to ensure that the quality of the service meets standards
- Data security: Organizations need robust security protocols and confirmation that their third-party service providers will comply with these protocols
- Communication & coordination: Organizations should have effective communication channels in place to make sure that everyone can work collaboratively with service providers; specially, offshore providers
- Risk management: Organizations need to establish effective risk management strategies to mitigate possible legal and regulatory issues

❖ Information as a Service (INaaS)

The capability provided to the consumer is to provide a simplified, integrated view of real-time, high-quality information about a specific business entity

Organizations can capture, organize, integrate, transform, analyze, and use information that can be incorporated with:

- Content management:

Enterprise Content Management (ECM), Web Content Management (WCM), Document Management (DM), Records Management (RM), Image Management, Workflow/Business Process Management (BPM), and Digital or Media Asset Management

- Documents created, updated & shared easily in an organized environment
- Information across the company will be managed in a single, secure repository
- Better decision making
- More direct access to documents
- Documents saved and delivered automatically
- A centralized repository for all information assets

- Business Intelligence (BI) tools

- Relational Databases

❖ Network as a Service (NaaS)

The capability provided to the consumer is to consume and optionally outsource the full lifecycle of the enterprise network deployment, with all hardware, software, licenses, and services (day-to-day operational

management of the network, including software upgrades, monitoring and troubleshooting, as well as decommissioning and end-of-life support) delivered in a flexible subscription-based offering, which can be accounted for as an operational expense.

Through this process, organizations get access to the latest and greatest technology while easing the burden on their IT staff

When do you need NaaS?

- Network hardware is due for a refresh, and the organization is lacking the performance it needs
- Improve security posture as more people, endpoints and devices connect to network, locally and remotely
- Struggling to manage a mixed-technology network environment that includes legacy components, interoperability issues between sites and regions, multiple service providers and inconsistent SLAs
- Adopting more IoT devices and sensors which need a network infrastructure that supports the low-latency (low inactivity), and time-sensitive nature of devices / sensors
- Struggling to find and retain the skills needed to service technology needs

Choosing a NaaS partner:

- A service provider should manage both the current state of network and its evolution: They should also be able to incorporate the latest network technology, including improved security, analytics and AIOps
- Work with one vendor: This can minimize contract complexities and eliminate a lack of interoperability between vendors and the need to maintain multiple software versions
- Adopt the NaaS model to save time and money: The flexibility to scale up and down as a major benefit, followed by supply chain certainty, accessing a catalogue of services from a single source, and a balance between operational and capital expenditure

NaaS advantages:

- Flexibility: Changes are made to the network via software, not hardware. IT teams are often able to reconfigure their corporate networks on demand
- Scalability: Enterprise NaaS customers can simply purchase more capacity from a vendor instead of purchasing, plugging in, and turning on more hardware

- Access from Anywhere: Depending on how a cloud-based network is configured, users may be able to access it from anywhere and on any device without using a VPN (Let's NOT forget strong access control). Ideally, all a user needs is an Internet connection and login credentials

- No Maintenance: The cloud provider maintains the network, managing software and hardware upgrades

- Bundled with Security: NaaS makes it possible for a single provider to offer both networking services and security services like firewalls. This results in tighter integration between the network and network security

- Cost Savings: Cloud customers do not need to purchase and maintain hardware, and the vendor already has the servers they need to provide the service

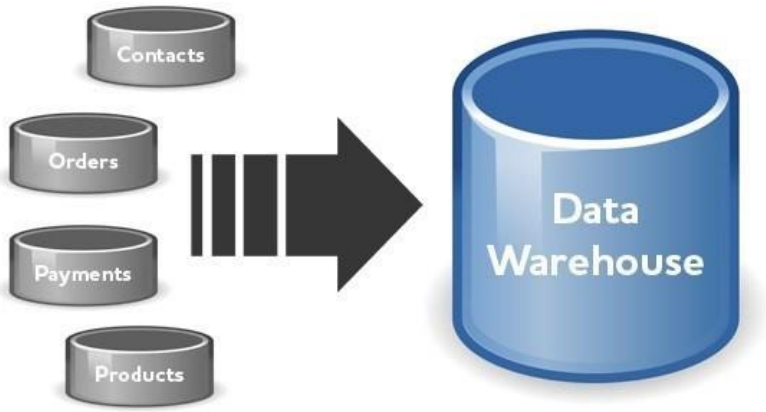
NaaS challenges and risks:

- Compatibility: The NaaS vendor's infrastructure may not be compatible with legacy systems that are still in place (older hardware, on-premises-based applications, etc.)

- Legacy Data Centers: In many enterprises, important applications and processes still run in on-premises data centers, not the cloud. This makes migration to a NaaS model slightly more challenging

- Vendor Lock-in: Moving to a cloud service always introduces the risk that an enterprise may become too reliant on that particular service provider. If the service provider's infrastructure fails or if they raise their prices, vendor lock-in can have major repercussions

❖ Data Warehouse as a Service (DWaaS)



Data Warehouse as a Service (DWaaS)

The capability provided to the consumer is to outsource the hosting, configuration, and managing all the required hardware and software for a Data Warehouse (DW). The customer provides the data and pays for the service

Cloud data warehouses are similar to on-premises ones from an architecture and technology standpoint:

- DBMS: A data warehouse requires a database management system (DBMS) to store, process and access the data it contains
- Data Storage: Data storage devices are provided
- Metadata Management Tools: Metadata characterizes data (answers the who, what, when, where, why and how questions for users of the data)
- Data Pipelines: Data warehouses are designed to support business intelligence (BI) and data analytics uses. Transaction data must be moved from operational systems into a data warehouse; the data also needs to be transformed to better organize and format it for analytical querying. Data integration tools that support extract, transform and load (ETL) or extract, load, and transform (ELT) processes are therefore required DWaaS components
- Reporting & Analytics Tools: BI tools that support querying, analytics and reporting functions against the data warehouse are thus a must

DWaaS advantages:

- Lower IT Costs: DWaaS eliminates the need for capital expenditures on hardware and software and decreases operating costs in on-premises data centers
- Easier Scalability: DWaaS users can quickly add more data processing and storage capacity when necessary and scale their systems back down when resources are no longer required. In addition, that can be done without the need to add or upgrade hardware or to continually renegotiate contract terms and conditions
- Reduced Staffing Needs: Because administration and management are mostly done by the service provider, an organization doesn't need to add new workers to support a data warehouse
- Faster Access to New Software Features: Instead of having to wait for a new release of a vendor's data warehouse software and then install it, as in on-premises systems, users can take advantage of software updates that DWaaS vendors often make on an ongoing basis

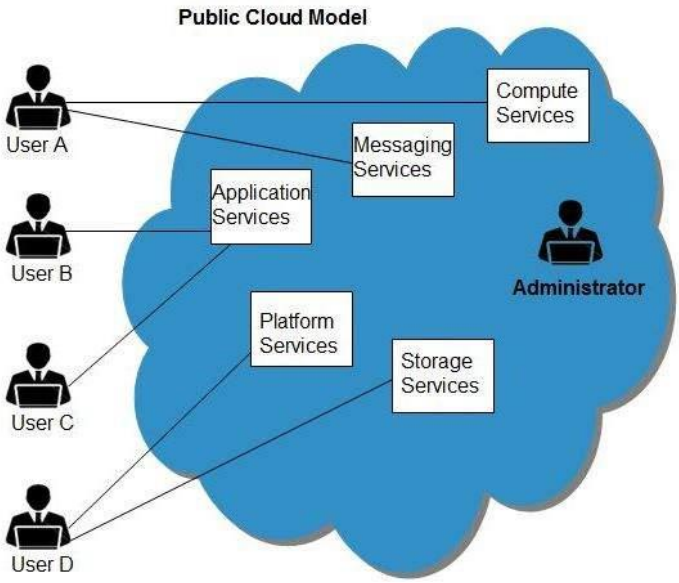
DWaaS challenges and risks:

- Performance & Availability: DWaaS requires a reliable internet connection. Customers have to rely on the DWaaS vendor to manage performance and ensure high availability
- Data Integration: The delay in getting data from operational systems into the data warehouse
- Analytical Queries that return large amounts of data are most at risk for data latency issues
- Vendor Lock-in: It isn't always easy to move from one DWaaS provider to another (every offering is different). It is wise to choose a DWaaS system with underlying components that your IT and data management team is knowledgeable about to help preserve the ability to migrate to another provider at a future point in time
- Security, Regulatory Compliance, & Risk Assessment
- Cost: Cost can also become an issue if use of a cloud data warehouse exceeds expectations or if unneeded system resources aren't identified and removed

Types of Cloud Computing

Deployment Models

- Public Clouds



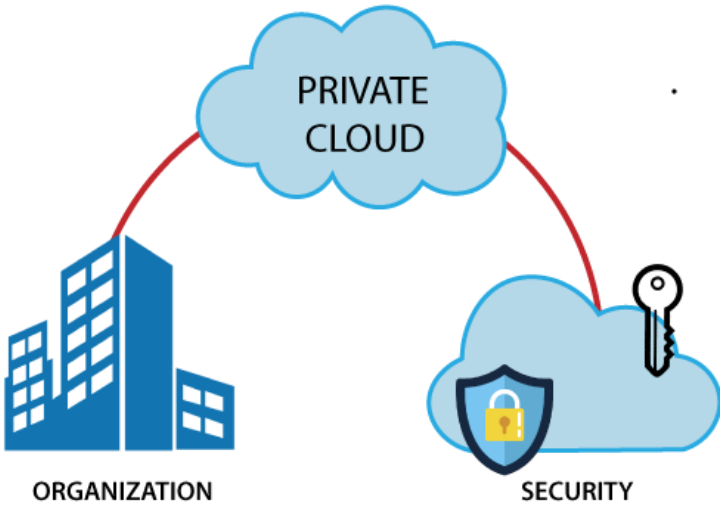
The consumption of public cloud services is almost via the Internet rather than a private or restricted network
Cheapest option available on the cloud infrastructure and it is available to everybody

Terms and conditions are mostly unilaterally decided by the cloud provider and the cloud consumer has very little say in this

Little significant responsibility is assumed by the cloud provider either on the availability or on the security of the information

Best for new organizations with no critical data that are looking for a cost-effective solution
Consumers can request higher service levels and higher assurance, but these come at a higher cost

❖ Private Clouds



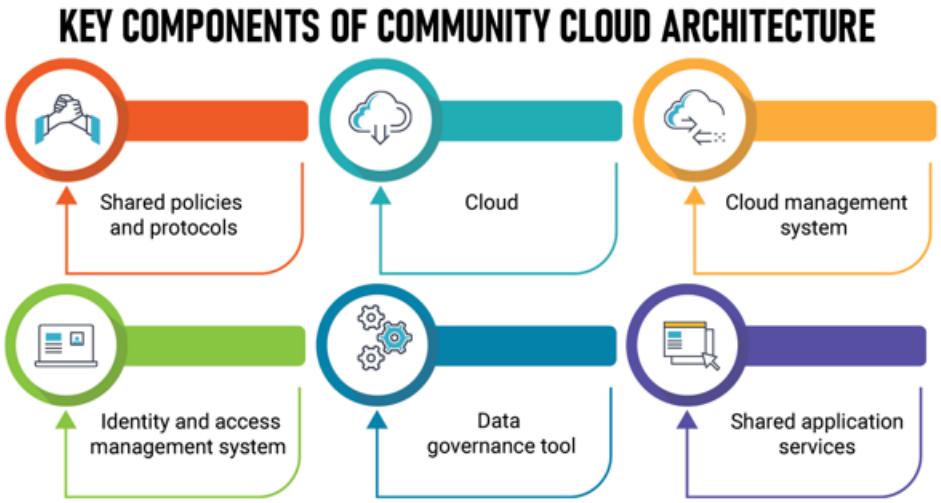
Dedicated and set up for a particular cloud consumer based on their unique high-security needs
High capital investment / high maintenance cost

High availability, confidentiality of the data, and complete integrity of the data

Consumer still has significant control over the cloud infrastructure

Security can be demanded by the consumer and can be provided by the cloud provider

❖ Community Clouds

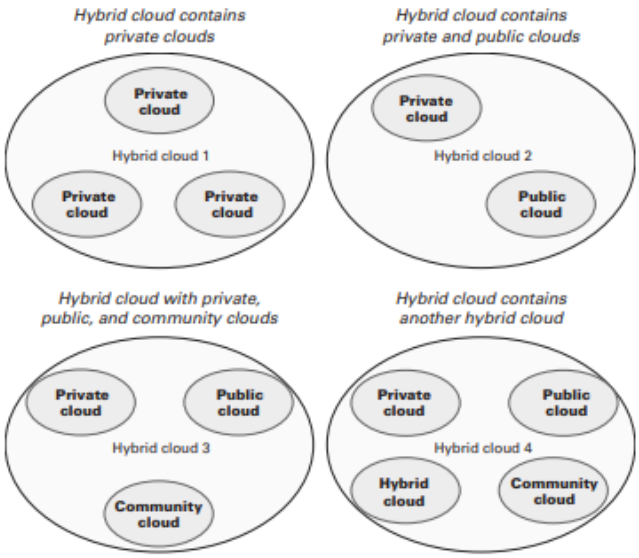


Set up for collaborative work between the organizations belonging to a particular community (health care, government organizations, or social service organizations) with shared objectives

May be managed by one or more of the organizations belonging to the community or may be managed by a designated outsourced agency or a third-party cloud provider

Information security may be still a concern as many organizations will be using the cloud

❖ Hybrid Clouds



A combination of any of the other deployment models

Highly critical and highly confidential applications may go on to private cloud while non-critical, non-sensitive, generic applications may go on to public cloud and community collaborations may be serviced through community clouds

Types of Clouds

❖ Personal Cloud

This cloud's scope is a person or a single entity and that it can be a private, public, or hybrid cloud (Public Personal Clouds: iCloud, Google Drive, Dropbox – Private Personal Cloud: network attached storage device that backs up data)

❖ Cloud of Things

A cloud of things has non-living objects, or things, as its scope; that is, it is a cloud that works with things instead of people or organizations (Public Lighting, Cars, Houses & Appliances, Offices, Health Monitoring Equipment)

NOTE: The pay-per-use charging mechanism could be provided through the agency of chip-and-pin technology that is available with most credit and debit cards

Cloud Computing; A Paradigm (Pattern) Shift?

NOTE: cloud computing is an enabling technology that bypasses many functions provided by your computer, the software installed on it, your workplace's IT and finance departments, businesses and government departments

Social Paradigm Shift

How you spend your leisure and how you live, both at a personal and a societal level
How that social life could be affected by cloud computing

Societal (Community) Clouds

Remember: A societal (Community) cloud is one that serves a group of people that have something in common; geography, hobbies, languages, or interests

The membership of the societal cloud would be defined by the common element you possess

An international societal cloud could be defined for NATO, UNO, EU …etc. The citizens of countries belonging to an international body would then be members of that cloud

Common benefits or issues could be considered by the cloud members; discussion boards, instant messaging, storage of shared documents, and video conferencing (All in a secure environment) – Example of PaaS societal cloud

A national societal cloud could exist for health care, training, politics, farming …etc.

The data collected could be de-personalized and aggregated to provide trend analyses

Example; in health care, the information collected with regard to a particular disease could be analyzed in terms of its concentration in particular areas, age groups, and social or income brackets, in real-time and an automated manner. The range and dispersion velocity of infections could be gathered from such a medical cloud to predict the spread of a disease across a country or region

Personal Cloud (Societal Cloud)

Personal files, music, pictures, streaming videos & clips

Health Wallet: information on doctors visited, results, medical costs, immediate alerts on health conditions using hooked devices

Financial statements, credit cards transactions, balance sheet and budget, investments

Cloud of Things

Home; information from a number of sensors related to security, smoke, proximity, light, and also automatically control curtains, fire alarms, lighting, and heating

Work Paradigm Shift

Workstations (laptops and desktops) are being replaced by machines that do not have applications installed on them - ***zero clients*** if they have the operating system embedded on the silicon chips or thin clients if they require an operating system on disk

Ubiquitous computing is much more than BYOD; it means that you can compute and access corporate information from anywhere, not only from the campus or the workplace, by using any device and at any time

NOTE: The IT department increasingly becomes a cloud service broker that maintains a service catalog of allowable cloud computing applications for an employee to use for work purposes

Organizational & Business Paradigm Shift

The IT department's function will evolve to one that maintains cloud service contracts with cloud service providers, whose services would be listed and described in a cloud service catalog that the IT department would maintain

Price & Value Models

Every price model starts its life as a ***cost model*** (a financial model that the cloud service provider creates to find out how much money to outlay on a particular cloud service in creating it, operating it, and then refreshing it to newer technologies after three years)

NOTE: Three years is the usual life span of technology before it becomes outdated, and five years is generally the absolute maximum the cloud provider will have before replacing the technology

The cost model will include:

- Inflation
- exchange rate variations (if applicable)
- depreciation
- electricity costs (these can be significant because of the power and cooling required by a large number of servers)
- floor-space costs
- software license costs
- labor costs
- capital costs to buy and operate servers

NOTE: Margin and a factor for risk are added to the sum of all the costs to arrive at a price

Utility Price Models

Utility models are metered price models whereby usage of the service is monitored, and you pay accordingly

- Consumption-Based Price Model
  - a commonly used model for IaaS and PaaS (pay for the computing resources that you use)
    - amount of storage (in Megabytes or Gigabytes)
    - computing or processing power (in terms of CPU cycles or number of processor cores used)
    - memory (in Megabytes or Gigabytes)
  - an average consumption rate of these resources is computed over a day, week, or month and you pay for the average utilization
  - for the cloud service provider, there could be other components that contribute to the cost of providing the service such as application licenses, data gathering, and maintenance costs

- Transaction-Base Price Model
  - transactions can be business related, such as invoices processed for an invoicing BPaaS, data related for INaaS, or application related for SaaS
  - cost of a transaction is calculated by dividing the cost of providing a cloud service by the estimated transaction volume over a given period (***unit transaction price***)
  - suitable under the following circumstances:
    - Transaction volumes are known and predictable
    - Business process can be defined clearly and can be measured in discrete units to represent a transaction
    - The transaction volume is tied to cost drivers
    - From the cloud service provider's perspective: when business processes are standardized and driven by transactions

- Subscription-Based Price Model
  - a fee, usually monthly, in order to use a service (regardless of whether those allocated resources are used)
  - should be decided to no longer use the service, you would need to provide a notice three months beforehand
  - can be used well for all cloud deployment models

- Service-Based Price Model
  - uses the benefit delivered to you, such as the SLA realized, risk transfer, or money saved, as the criteria for defining the price you pay for the cloud service

- Fixed Price Model
  - the price for this service is fixed on a yearly, quarterly, or monthly basis
  - is usually used to transfer risks related to delivery, people and quality
    - The risk transferal occurs through the SLAs that define and agree with the cloud service provider

- Volume-Based Price Model
  - can relate to:
    - number of users
    - amount of storage space
    - speed of transactions (denoted as number of transactions per minute or hour)
    - amount of bandwidth
    - processing power utilized
  - because volume varies over time, the price periodically changes
  - most often used in IaaS and PaaS

- Tiered Price Model
  - uses a tiered (level) form of pricing that is based on SLAs, volume, or amount spent
  - can apply with greater discounts provided that you spend a certain amount each year
  - tiers based on the SLAs such that the more stringent the SLAs, the more you pay

Performance Price Models

- Outcome-Based Performance Price Model
  - provide a bonus if an outcome is achieved
  - often used with other models, usually fixed price models, in order to create a value culture based on rewards

- Gain-Share Performance Price Model
  - instead of having penalties should certain SLAs not be met, you reward the service provider by sharing your profits if the SLAs are exceeded
  - can combine the gain-share model with a penalty-based performance model to create a hybrid performance model

Marketing Price Models

- Freemium Marketing Price Model
  - try before you buy a more enhanced service
  - get a free service but with advertisements
  - suited to SaaS because many software companies such as LinkedIn and Dropbox use it well
  - the idea is to offer enough value to users in the free version in order to attract and retain users, and more value in the enhanced version to ensure that the users convert and maximize the service provider's revenue
- Razor-and-Blades Marketing Price Model
  - a device or an app that uses a cloud service may be given away, but the price may be made up from the data that is stored, analyzed, and presented by the cloud service

Security & Governance

What is IT Security?

NOTE: IT security protects the confidentiality, integrity, and availability (CIA) of computer systems and the data they store or handle from unintended use

The CIA security attributes have evolved into six that are known as "***Parkerian Hexad***"

- **Confidentiality:** who can get what kind of information
- **Possession or control:** who and what systems possess the information or have control over its use
- **Integrity:** refers to the information being correct or consistent with its intended use. Any unauthorized modification of data, whether deliberate or accidental, is a breach of data integrity
- **Authenticity:** refers to the veracity (legitimacy) of the information's origin or creation
- **Availability:** refers to having access to the information in a timely manner, when it is required for its intended use
- **Utility:** refers to usefulness: having the information in a usable and useful manner so that it can be used as intended by the intended user

Availability

Remember: One of cloud computing's characteristics is ubiquity (universal), which offers the availability of cloud computing resources

Features of Availability:

- Will a service be available from any other location? (***Should be defined in the contract with cloud service provider***)

- How readily will it be available when you want to use it? (***Should be defined in the contract with cloud service provider***)

- Will there be certain times when it may not be available because of planned maintenance? (***Expressed as a percentage***)

- If the cloud platforms hosting the service were to go down, how long would it take to recover? (***Recovery Time Objective – RTO – expressed in time unit***)

- Once recovery is complete, will I have lost any data and, if so, how many hours' worth of data will it be? (***Recovery Point Objective – RPO – expressed in time unit***)

NOTE: Availability metrics should be measured and defined as SLAs that then form part of contractual agreement with the cloud service provider

Each of the CIA or Parkerian attributes can be given numeric values to denote its severity and each of the severity levels can be explained

Example:

1. Low Severity
2. Medium Severity
3. High Severity

So, a security requirement for the CIA could be expressed as 1-3-2

AND

A security requirement for the Parkerian Hexad could be expressed 2-3-2-1-3-1

Enforcing Security

NOTE: An IT security breach can be described in terms of the six attributes of the Parkerian Hexad

If we were to follow the data trail, the data would originate from a *user*, pass over a *network* to reach a *computing system* that hosts *software*, which processes the data and stores it in a *storage device*, such as a solid-state disk, and that data gets backed up onto a *backup device* and finally, after a period of time, gets archived in an *archival system*

Each of the elements in the data journey described must share the same security characteristic in terms of the CIA triad or the Parkerian Hexad in alignment with the user's requirements

Data transiting from one element to another need to be secured, so the channels that enable such data transfers must also be made secure

Security Containers

Security Container: All those elements within the cloud computing environment that share the same security characteristics for a particular user can have a common security boundary

Rather than define security boundaries for each elements that have touch points with data, ***segmentation*** (takes place at the network layer) is generally used to create a container, which then contains the elements that share the same security attributes

Virtual networks are created (exist on a physical network) and each container uses virtual networks inside it so that other containers (outsiders) cannot have access to its internal data

In order to enter a particular container, three security procedures are normally used: identification, authentication, and authorization

Thus identification asks “who are you,” authentication asks “are you who you say you are,” and authorization asks “what are you allowed to do within the cloud computing environment.”

Monitoring

The first defense mechanism that is employed to deter security breaches is a firewall

A number of firewalls would be placed at the boundary of every security container

Remember: The cloud itself, being a security container, will therefore have an outer firewall

The firewall will contain rules that tell it what traffic to allow through and what traffic to block. You can be alerted if someone tries to enter a security container and is blocked by the firewall. The alert can be an email or an entry in a log file that can be monitored

However,

A security system will have a number of components; firewalls, user authentication and identification, intrusion detection and prevention, and user-based security such as anti-virus and anti-malware tools

Such a system, if properly configured, will generate logs that will keep track of users, services provided to the users, and data

Software is used to analyze the server and firewall logs, as a first step in monitoring, in order to detect any suspicious activity

The second line of defense is at the user authentication and identification stage. If a number of failed attempts are made to log in as someone or to a particular service, then the monitoring tools ought to alert the cloud system administrator

If the tools are automated, then they may deny further logins on that account or to that service by the username concerned

The client devices (third line of defense) need to be protected against malicious attacks so that user log-in details may not be compromised in order to access cloud services

Cloud Security Challenges

- **Lack of visibility**: Since many cloud services are accessed outside of corporate networks and through third parties, It's easy to lose track of how data is being accessed and by whom

- **Multitenancy**: Public cloud environments house multiple client infrastructures under the same umbrella, so it's possible your hosted services can get compromised by malicious attackers as collateral damage when targeting other businesses

- **Access management and shadow IT**: It is dangerous for organizations that don't deploy bring-your-own device (BYOD) policies and allow unfiltered access to cloud services from any device or geolocation

- **Compliance**: Regulatory compliance management is oftentimes a source of confusion for enterprises using public or hybrid cloud deployments. Overall accountability for data privacy and security still rests with the enterprise, and heavy reliance on third-party solutions to manage this component can lead to costly compliance issues

- **Misconfigurations**: Misconfigurations can include leaving default administrative passwords in place, or not creating appropriate privacy settings

Available Cloud Security Solutions

- **Identity & Access Management (IAM)**
  The core functionality of IAM is to create digital identities for all users so they can be actively monitored and restricted when necessary during all data interactions

- **Data Loss Prevention (DLP)**
  DLP solutions use a combination of remediation alerts, data encryption, and other preventative measures to protect all stored data, whether at rest or in motion

- **Security Information & Event Management (SIEM)**

Using artificial intelligence (AI) – driven technologies to correlate log data across multiple platforms and digital assets, SIEM technology gives IT teams the ability to successfully apply their network security protocols while being able to quickly react to any potential threats

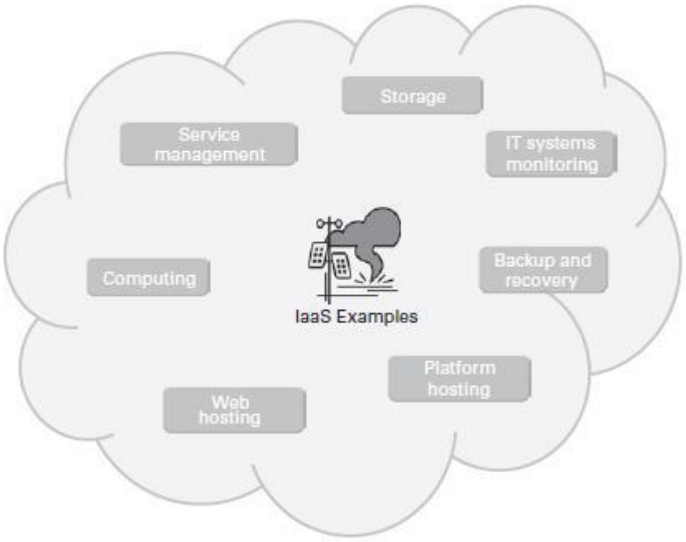
- **IBM X-Force Red**

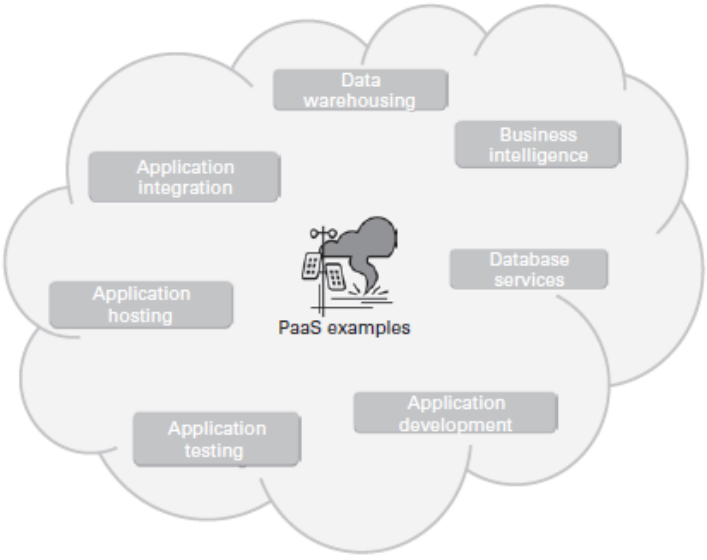
Uses the same tactics, tools, techniques and mindsets as attackers to uncover & help organizations fix vulnerabilities

Use Case for IAAS & PAAS

In cloud computing, the IT infrastructure is grouped into two distinct granularities (distinguishable pieces)

- All the physical devices such as the server, network, storage, and computing device, are denoted “infrastructure.” Hence the IaaS
- When the servers and computing devices are combined with their operating system and middleware, they are referred to as “platform.” Hence the PaaS





Web Hosting

Characteristics of website hosting:

- You have very little sense of the traffic
- The traffic can vary by time of day, week, or month
- There can be bursts of traffic when a marketing campaign or a product launch occurs

These characteristics are in addition to the general requirement for infrastructure to scale as the business expands

The IaaS/PaaS cloud computing model is ideally suited to address these needs of web hosting because of its elasticity and usage-based pricing model

Storage

The storage normally provided by IaaS or PaaS providers has built in redundancy on redundant arrays of inexpensive disks (RAID)

IaaS based cloud storage solutions are ideal since they are readily available, have usage-based price models, can be accessed from anywhere in the world, and can be accessed using any device

Most commercial offerings for storage are Apple's iCloud, Dropbox, Google Drive, and Amazon S3

Backup & Recovery

The cloud service-based backup would have a backup location that different from that of users

The disadvantages of the cloud-based backup:

- Risk of a security breach at the cloud service provider whereby a third-party can obtain your data
- Employees of the cloud service provider having access to your data

NOTE: One way to overcome these disadvantages is to use a strong encryption mechanism and backup the encrypted files

It would make sense to appoint a different cloud service provider for backing up some or all of your data that is stored on another cloud service provider

A form of integration, or a simple application to backup and restore, would be needed between the two cloud service providers to ensure unrestricted data flow

One way to achieve this would be to synchronize the data between the two repositories using software such as freefilesync

Database Services

"Database as a Service" - hosted on PaaS - ensures that you have a cloud cell that acts as a database system

A database service would need to be accessible easily and quickly for the applications that need to use it. Ideally you would want the database service to be in the same cloud as the applications that access it. This minimizes transaction times and provides optimum performance

The advantage of such a configuration is that you would have most of the IT stack in the cloud: the application, its database, and its physical storage. Another advantage is databases' usefulness for a variety of applications

A database service could be configured as a cloud cell that acts as an appliance. This means that every time you needed to have a database, you would not need to specify, install, and configure one; you would instead just call up the database cloud cell within your cloud environment and link it to your application

Application Development

Advantages to using PaaS for application development:

- Enables you to focus on creating the application, not peripheral things like the hardware
- With the consumption-based price model you do not have to pay for the infrastructure up front
- You can create applications that scale from one to upward of a million users without having to re-architect your application
- Components such as storage and databases are available as standard, ready-made, off-the-shelf services for your application to use
- You are provided with a standardized development environment that is familiar to most application developers. This can additionally include an application framework, code samples and development tools

Commonly used cloud platforms currently are Microsoft's Azure, Google's App Engine, and Amazon's Elastic Compute Cloud (EC2)

Application Testing

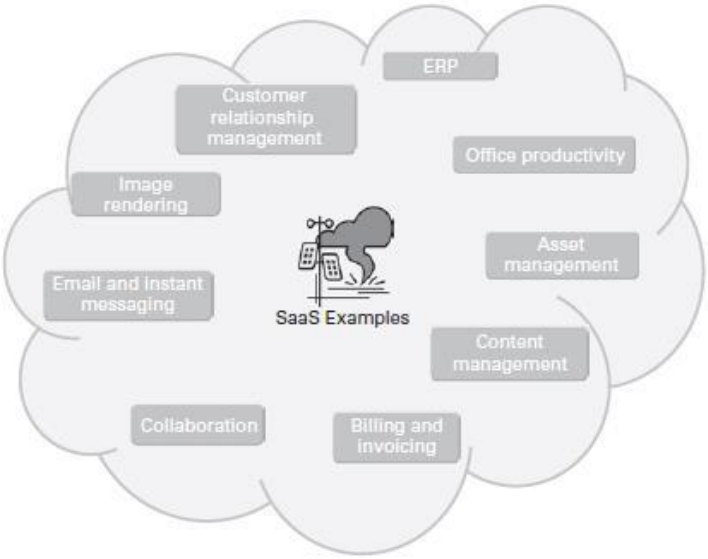
Testing serves two purposes: it validates the user requirements are right for the application, and it verifies that the application meets those requirements.

The main benefits of using cloud services for testing:

- Test environment can double up as a demo environment.
- Flexible testing environment available without any capital costs
- Flexibility to ramp up or down as your testing needs change
- Ease of migration between multiple environments (demo, development, testing, etc.)
- Standardized test tools, procedures, and test scripts if environment is shared with your client; this is especially useful for beta and user acceptance testing
- Agility to go to market as timescales for setting up test environments are reduced
- Software sizing and volumetric information gained from simulated users help to assess scalability and infrastructure needs

You can use the cloud-based test environment to perform various tests. Disaster recovery tests, functional tests, integration tests, load tests, operations tests, performance tests, stress tests, security tests, system tests, unit tests, and user acceptance tests

Use Case for SaaS



NOTE: In cloud computing, any software that runs in the background for supporting integration and monitoring purposes is termed middleware, and not “software”

CRM

CRM helps to manage a company’s interactions with current and prospective customers. Also, it provides reporting and dashboards to assess various customer growth

Commonly available CRM SaaS offerings are Microsoft Dynamics and Salesforce CRM

Advantages of using an SaaS-based CRM solution:

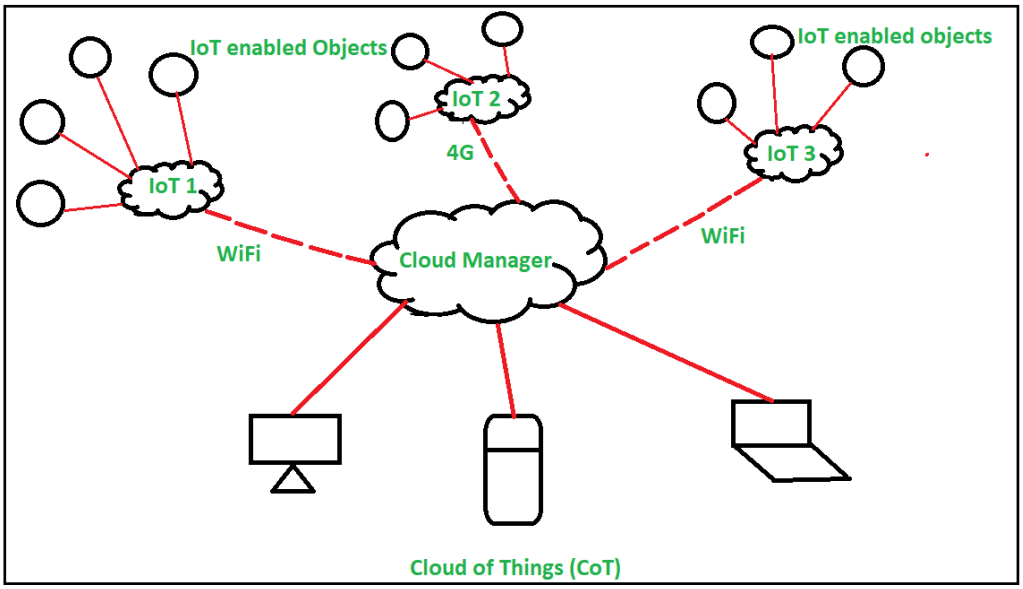
- Ability to access customer records from anywhere in the world
- Ability to track and assess sales team’s performance in a standardized and objective manner
- Have an instant idea of revenue growth profile

Office Productivity

Microsoft provides Office 365 for you to use from the cloud, and Google provides Google Docs, Sheets, and Slides that let you create online documents, work on them in real time with other people, and store them in your cloud storage online

Future Outlook

Cloud of Things & Services (CoTS)



NOTE: The key principle of CoTS is automation. This supports the dual principles of IoT and

IoS: convenience and service when and where needed

Broad areas where CoTS based services can be provided:

- Smart home: Nest smoke detector and fire alarm system are examples of connected devices within the home or office
- Wearables: Google Glass and Apple iWatch are good examples of these. They provide a platform not only for communication but also for sensors to monitor your health or environment
- Smart city: Traffic management, water distribution, waste management, urban security, environmental monitoring, pedestrian congestion management, and street lighting are some example use cases of connecting a CoTS service to IoT devices
- Smart grids: Smart metering augmented with IoT services for information about electricity consumption to improve the efficiency, reliability, and economics of electricity usage
- Retail: Proximity-based advertising and smart wallets
- Healthcare / Farming / Transportation

Cloud Service Level Agreement

According to ITIL (Information Technology Infrastructure Library):

A **Service Level Agreement** (SLA) is a formal, negotiated document that defines (or attempts to define) in quantitative (and perhaps qualitative) terms the service being offered to a customer. Any metrics included in a SLA should be capable of being measured on a regular basis and the SLA should record by whom

A **Contract** is a legally binding agreement between two or more parties. Contracts are subject to specific legal interpretations

---

As consumers move towards adopting such a Service-Oriented Architecture, the quality and reliability of the services become important aspects

The demands of the service consumers vary significantly

It is not possible to full all consumer expectations from the service provider perspective and hence a balance needs to be made via a negotiation process

At the end of the negotiation process, provider, and consumer commit to an agreement; SLA

Remember: SLA serves as the foundation for the expected level of service between the consumer and the provider. The QoS attributes that are generally part of an SLA (such as response time and throughput) need to be closely monitored

Cloud SLAs may be more detailed to cover governance, security specifications, compliance, and performance and uptime statistics. They should address security and encryption practices for data privacy, disaster recovery expectations, data location, as well as data access

A Cloud SLA outlines intervals for reviewing a contract so that it meets the changing needs of an organization

A Cloud SLA should also define compensation for users if the specifications aren't met

A Cloud SLA should include an exit strategy that outlines the expectations of the provider to ensure a smooth transition

The 5 Topics that should be looked at in SLA:

- ❖ Availability
  - The biggest quality-of-service (QoS) concept
  - Providers might break down availability depending on time frame – for example, they might promise 99.99% availability during business hours
  - Provider's plan for unexpected downtime, including alerting its users and providing updates on maintenance and service repairs

- ❖ Data Ownership

Who owns your data in the cloud?

  - SLA should specifically outline its data ownership policies so that everything is transparent and clear
  - If the provider doesn't explicitly state its data ownership policies in the SLA, you can't guarantee the safety of your information

- ❖ Cloud H/W & S/W
  - The provider should outline the hardware that the cloud services rely on, including servers and other devices (will help you understand the specifics behind your cloud environment's construction. and what you'll need to educate your staff on)

- ❖ Disaster Recovery & Backup
  - Cloud providers should have a section of the SLA that describes their disaster recovery and backup solutions in detail
  - Depending on the provider, they may provide automatic backups and snapshots of your data
  - If the user is required to set up backup and recovery systems, the SLA should outline that (It may not specifically state how to activate them, but you should be aware if you need to activate them or not)

- Customer Responsibilities

  - Cloud provider needs to inform you of what you're liable for when you enter the agreement

  - Make sure you mull over the entirety of the SLA to know what your provider will manage and what you need to as a customer

Cloud SLA Lifecycle

1. Acquisition

Phase I: Assessment

❖ Evaluate a Cloud Service Security Attributes

- **Authentication & Identity**

  - **Multi-Factor Authentication**: Does the cloud service support authentication factors in addition to passwords such as an SMS code or phone token?

  - **Anonymous Use**: Does the cloud service provider allow for anonymous access to the service?

  - **Identity Federation Method**: What single sign-on methods does the cloud service provider support?

  - **Enterprise Identity**: Does the cloud service provider support integration with enterprise directories or authentication providers?

- **Protection for Customer Data**

  - **Encryption of Data at Rest**: Does the service encrypt data at-rest in its databases, file systems or at the virtual machine layer?

  - **Encryption of Data in Transit**: What mode of SSL or TLS does the vendor support for protecting data in motion?

  - **Data Multi-tenancy**: Does the cloud service provider support a multi- tenant offering?

- **Internal Controls**
  - **Certifications**: Which compliance certifications does the cloud service provider have (e.g., ISO 27001, etc.)?

    ISO 27001 provides a framework to help organizations, of any size or any industry, to protect their information in a systematic and cost-effective way, through the adoption of an Information Security Management System (ISMS)

    The basic goal of ISO 27001 is to protect three aspects of information: CIA

An Information Security Management System (ISMS) is a set of rules that a company needs to establish in order to:

- ✓ identify stakeholders and their expectations of the company in terms of information security
- ✓ identify which risks exist for the information
- ✓ define controls (safeguards) and other mitigation methods to meet the identified expectations and handle risks
- ✓ set clear objectives on what needs to be achieved with information security
- ✓ implement all the controls and other risk treatment methods
- ✓ continuously measure if the implemented controls perform as expected
- ✓ make continuous improvement to make the whole ISMS work better

This set of rules can be written down in the form of policies, procedures, and other types of documents, or it can be in the form of established processes and technologies that are not documented

---

- **Data center protections**: Does it have data center protections?

- **User Activity Logging**: Does the cloud service provider log end-user activities?

- **Legal Terms**

  - **IP Ownership**: What are the specified definitions of intellectual property ownership in the terms of use for the cloud service provider?

  - **Account Termination**: What are the grounds for account termination with the cloud service provider?

  - **Data Retention**: How long does the service store customer data after account termination?

  - **Data Sharing Policy**: Does the service reserve the right to share customer data with third parties, and if so under what circumstances?

❖ Past Performance

- **Known Breaches**: Has the cloud service provider had a (publicly disclosed) breach in its service?
- **Known Malicious Use**: Is the cloud service provider known to have (publicly disclosed) malware hosted on its site or known to be a drop zone for malicious code?
- **Penetration Testing**: Does the vendor perform penetration testing on a regular basis?

❖ Support

There is an increasing attention by providers to customer support. The offer of 24/7 support is a differentiator used by leading Cloud Service Providers with AWS (Amazon Web Services) leading the trend

❖ Standards & Certifications

Standards and security certification schemes play a key part in building trust, helping prospective customers to better compare cloud service offers also from a security point of view

Trust is increasing in importance as more and more mission-critical workloads move to the cloud. It is vital that companies have confidence in the ability of their cloud service to support the needs of their business, while also providing value for money

❖ Market Structure & Cloud Pricing Models

It is important that customers keep pace with the market price of the basics, and use them as a foundation to up-sell higher margin, value-added services

Phase II: Preparation

This phase includes the first contact and conversation with possible CSPs, further assessment, pre-evaluation and fine-tuning goals and assumptions. Based on the cloud service, customers can rate risks, opportunities and security to understand the main features of the cloud service under deployment; Management of h/w, s/w, updates, backups; Geographic Spread; Elasticity; Incident Response; Unexpected Costs; Vendor Lock-In; Foreign Jurisdiction

Phase III: Negotiating & Contracting

From the very beginning, it is very important to clarify the specific responsibilities of each party, whether shared or individually owned. Taking these steps means you can mitigate the risk of losing key protections and efficiencies that SLAs can provide

Before implementing a cloud contract, both parties should make an exhaustive review and negotiation of the service level agreements, wherever this is possible

Agreements with the provider should include SLAs that not only benefit the vendor but also safeguard your business or agency, so clarify the specific responsibilities of each party, whether shared or individually owned. Define penalties with documented credit amounts for each missed deliverable

Pay special attention to the termination phase during negotiation, as conditions prove critical in protecting against cloud vendor lock-in. Ensuring all conditions are properly in place gives you, the customer, and greater control over the cloud services you are using

NOTE: Some service providers sell through indirect channels via partners. This means the SLAs and associated contract is signed between the partner and the final end-user. This may (or may not) leave room for negotiation

2. Operation

It determines whether a cloud service meets the committed service level objective (SLO) during the provisioning of the cloud service. This might imply that cloud service providers taking corrective actions to avoid SLA violations

Why is it important?

SLAs can be used to monitor the cloud service provider in order to assess the correct fulfilment of the cloud service, or detect potential violations in which case remediation may take place

Phase IV: Execution & Operation

It includes the actual start of setting up the cloud services, populating the respective cloud service with relevant data, on boarding and training users, setting up communication channels and further operational activities while using the respective cloud services

❖ Performance Metrics

It is important to highlight the uptime or availability of service from a Cloud Service Customer perspective. This guarantee should be analyzed based on the type of service it applies, and most importantly to the type of business the service is essential. Otherwise it can be meaningless

Example:

99.95% monthly availability only permits about 21 minutes of downtime (and in most cases 99.9% with a 40 minute period of downtime), that can correspond to large money loss for a company if it happens during the most critical period for the business

While these percentages can be very promising for most of the business using the Cloud, it might be critical for a business that needs reliability of the infrastructure of the Cloud services in general to function correctly

The compensation of the CSP in such cases is only in service credit percentage

Phase V: Updates & Amendments

It is important that Cloud Service Customers carefully check how updates and amendments to their contract are made

Examples:

"To the Service Offerings. We may change, discontinue, or deprecate any of the Service Offerings (including the Service Offerings as a whole) or change or remove features or functionality of the Service Offerings from time to time. We will notify you of any material change to or discontinuation of the Service Offerings".

"We reserve the right and entitlement to alter the Agreement at any time. We will notify you in accordance with the Agreement at least thirty (30) days prior to any alterations becoming valid and binding."

"We reserve the right to change our prices at any time. Definitive pricing is available through the control panel at the time of purchase, and supersedes any information given here. Special offers may be subject to additional conditions. All prices are exclusive of VAT which will be added at the applicable rate. All services are offered subject to our terms and conditions."

"In order for CSP X to consider a Claim, Customer must submit the Claim to Customer Support within two months of the end of the billing month in which the Incident that is subject of the Claim occurs. Customer must provide to Customer Support all information necessary for CSP X to validate the Claim, including but not limited to detailed descriptions of the incident, the time and duration of the Incident, the affected resources or operations, and any attempts made by Customer to resolve the Incident."

"We will be the sole arbiter regarding the award of credit and our decision will be final and binding."

Phase VI: Escalation

It deals with contractual or other non-compliance, breaches, and other incidents during the term of the ongoing cloud services arrangements that have resulted in a dispute that needs escalation, (perhaps even litigation as a last resort), negotiation and resolution, either by parties themselves or by arbitration, court or otherwise

3. Termination

It includes the assessment of alternatives, settlement and termination arrangements, cloud services transition projects and services, data export, customer and end-use care and diligence, and adequate data deletion