
Certified Cloud Security Professional

# Official (ISC)² Student Guide

The CCSP student guide provides a comprehensive review of the knowledge required for understanding cloud computing and its information security risks and mitigation strategies.

An Official (ISC)² Publication

The Certified Cloud Security Professional (CCSP) training provides a comprehensive review of cloud security concepts and industry best practices, covering the 6 domains of the CCSP Common Body of Knowledge.

- Architectural Concepts and Design Requirements
- Cloud Data Security
- Cloud Platform and Infrastructure Security
- Cloud Application Security
- Operations
- Legal and Compliance

## The only global cloud and information security credential backed by the Cloud Security Alliance (CSA) and (ISC)².

CCSP®

Certified Cloud Security Professional

3rd Edition

ANSI ACCREDITED

ISO/IEC 17024
Personnel Certification
#0668

Dear Seminar Participant,

We are pleased that you have chosen to participate in (ISC)²®'s Official Certified Cloud Security Professional (CCSP®) CBK® Review Seminar. This comprehensive course will help in your review and deepen your knowledge of information security. Your efforts this week will go a long way toward attaining the CCSP credential.

This review seminar includes materials based on the latest version of the (ISC)² CBK, contributions from (ISC)²-authorized instructors and subject-matter-experts, as well as a post- seminar self-assessment. The latest security topics such as cloud computing, mobile security, application security, and more are regularly integrated into our courses through a rigorous process of evaluation and updates. By leveraging the course materials provided with the expertise of your qualified (ISC)² instructor and your own review initiatives, you are constructing the ideal study plan for the CCSP examination.

The time you invest studying for the exam is well worth the outcome. Information security is one of the most rapidly advancing fields in the world, and achieving (ISC)² certification is a great step toward enhancing your career and securing your future.

I wish you the best of luck this week and in your quest to achieve the CCSP certification!

Regards,

David P. Shearer, CISSP
Chief Executive Officer
(ISC)²

# Acknowledgement

The development of the CSSP Training Guide could not have been possible without the participation and assistance of so many people. Their contributions are sincerely appreciated and gratefully acknowledged.

Authors:
Kevin Jackson, CCSP
Melvin Greer, CCSP
George Murphy, CISSP, CCSP, and SSCP

Editorial Service:
Trey Wright
Elsa Peterson, Ltd. Editorial Services

Instructional and Graphic Design:
eLearning Mind (ELM)

Cover Design:
Jon Harrison, (ISC)²

# Table of Contents

# Welcome

The Official (ISC)®² Certified Cloud Security Professional (CCSP®) Training Seminar provides a comprehensive review of information systems security concepts and industry best practices, covering the six domains of the CCSP Common Body of Knowledge (CBK®):

- Architectural Concepts and Design Requirements
- Cloud Data Security
- Cloud Platform and Infrastructure Security
- Cloud Application Security
- Operations
- Legal and Compliance

This training course will help candidates review and refresh their information security knowledge as they pursue the CCSP certification.

## How Do I Use the Course Materials?

The CCSP Training Seminar course material is built using the topics from the Exam Outline and additional topics approved by the (ISC)² CCSP Education Committee. The seminar is broken into progressively smaller sections in support of the course objectives. Each domain header identifies the objectives and what a student can expect to learn after completing the domain. These objectives are divided into smaller modules and sections. Modules contain activities that reinforce covered topics with a goal to increase knowledge retention.

The workbook is designed to be a self/group study tool that includes activities, references to external reading resources, study questions, and a glossary of terms. The columns on the outside of the pages are intended to be a place to make notes. There are five icons in use throughout the book. The icons and their meaning is outlined below.

**Notes**

Welcome

**PPT**

**Welcome**

**PPT**

**How Do I Use the Course Materials?**

**Notes**

Welcome

**PPT**

**Course Objectives**

This icon identifies a related PowerPoint slide: **PPT**

It is important to note that information throughout the course is presented from two different viewpoints:

Cloud service consumer:

Cloud service provider:

Representative icons will help you identify these differing perspectives and will be used throughout the course materials.

This icon identifies a case study that will be presented and discussed during class time:

This icon identifies an activity that will be performed during class time:

## Course Objectives

After completing this course, the participant will be able to:

- Describe the physical and virtual components of and identify the principle technologies of cloud-based systems.
- Define the roles and responsibilities of customers, providers, partners, brokers, and the various technical professionals that support cloud computing environments.
- Identify and explain the five characteristics required to satisfy the NIST definition of cloud computing.
- Differentiate between various as-a-Service delivery models and frameworks that are incorporated into the cloud computing reference architecture.
- Discuss strategies for safeguarding data, classifying data, ensuring privacy, assuring compliance with regulatory agencies, and working with authorities during legal investigations.
- Contrast between forensic analysis in corporate data centers and cloud computing environments.
- Evaluate and implement the security controls necessary to ensure confidentiality, integrity, and availability in cloud computing.
- Identify and explain the six phases of the data lifecycle.
- Explain strategies for protecting data at rest and data in motion.
- Describe the role of encryption in protecting data and specific strategies for key management.

- Compare a variety of cloud-based business continuity/ disaster recovery strategies and select an appropriate solution to specific business requirements.
- Contrast security aspects of Software Development Lifecycle in standard data centers and cloud computing environments.
- Describe how federated identity and access management solutions mitigate risks in cloud computing systems.
- Conduct gap analysis between baseline and industry standard best practices.
- Develop Service-Level Agreements (SLA) for cloud computing environments.
- Conduct risk assessments of existing and proposed cloud-based environments.
- State the professional and ethical standards of (ISC)² and the Certified Cloud Security Professional.

**Notes**

Welcome

**PPT**

**Course Objectives (continued)**

# Course Agenda

| Domain 1: Architectural Concepts and Design Requirements |
|---|
| Cloud Data Security |
| Cloud Platform and Infrastructure Security |
| Cloud Application Security |
| Operations |
| Legal and Compliance |

## Notes

Architectural Concepts and Design Requirements Domain

**PPT**
**Course Agenda**

**PPT**
**Architectural Concepts and Design Requirements Domain**



# Domain 1: Architectural Concepts and Design Requirements Domain

## Welcome to the Architectural Concepts and Design Requirements Domain

### Welcome

The goal of the "Architectural Concepts and Design Requirements" domain is to provide you with knowledge of the building blocks necessary to develop cloud-based systems.

You will be introduced to cloud computing concepts with regard to the customer, provider, partner, measured services, scalability, virtualization, storage, and networking. You will also be able to understand the cloud reference architecture based on activities defined by industry standard documents. It is important to note that information throughout the course is presented from two different viewpoints:

Cloud service consumer:

Cloud service provider:

Notes

Architectural Concepts and Design Requirements Domain

Representative icons will help you identify these differing perspectives. This entire domain is from the consumer's perspective.

Lastly, you will gain knowledge in relevant security and design principles for cloud computing, including secure data lifecycle and cost-benefit analysis of cloud-based systems.

## Domain Objectives

After completing this domain, you will be able to:

- Describe the history of cloud computing.
- Define the various roles, characteristics, and technologies as they relate to cloud computing concepts.
- Describe cloud computing concepts as they relate to cloud computing activities, economics, capabilities, models, internet security, and cross-cutting aspects.
- Define the differences between enterprise IT, managed service providers, and cloud computing.
- Understand core cloud computing technologies.
- Describe and understand cloud computing reference architectures.
- Understand the importance of business or mission requirements when developing a cloud computing strategy.
- Understand the minimum components of a cloud computing migration strategy.
- Understand how to manage cloud computing risks.
- Understand the importance of enterprise governance in cloud computing.
- Understand information technology service management.
- Define the various design principles for the different types of cloud models.

# Domain Agenda

| Module | Name |
|---|---|
| 1 | History of Cloud Computing |
| 2 | Understand Cloud Computing Concepts |
| 3 | Cloud Economic Model |
| 4 | Cloud Computing Supporting Fund |
| 5 | Cloud Reference Architecture |
| 6 | Understanding the Business Requirements |
| 7 | Enterprise Cloud Computing Policies |
| 8 | Cloud Migration Planning |
| 9 | Domain Review |

## Case: Target

A data breach on or around Black Friday in 2013 compromised credit card details of about 110 million Target credit/debit-card holders. The attackers pilfered 11 gigabytes of data. Review these resources to learn about the incident and the importance of transitioning from an infrastructure-centric security model to a data-centric security model.

### Failure of IT Governance

*https://www.blackswangroup.com.au/news/the-target-breach*

### A "Kill Chain" Analysis of the 2013 Target Data Breach

*https://www.commerce.senate.gov/public/_cache/files/24d3c229-4f2f-405d-b8db-a3a67f183883/23E30AA955B5C00FE57CFD709621592C.2014-0325-target-kill-chain-analysis.pdf*

### Anatomy of the Target data breach: Missed opportunities and lessons learned

*http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/*

## Notes

Architectural Concepts and Design Requirements Domain

**PPT**
**Domain Agenda (two slides)**

**PPT**
**Case: Target**

**PPT**
**After the Breach**

Notes

History of Cloud Computing

PPT
**History of Cloud Computing**

PPT
**Module Topics**

# Module 1: History of Cloud Computing

## Module Topics

- Introduction
- Computing First Age
- Computing Second Age
- Computing Third Age
- Computing Today

# Introduction

Information technology has gone through important changes over the years. In order to understand where we are, it's important to understand where we have been. This short history will help you appreciate why cloud computing is fundamentally different than traditional IT.

# Computing First Age

For our purposes, the first age of computing was the 1970s, when the focus was on big infrastructure—mainframes, big point-to-point networks, centralized databases, and big batch jobs. Toward the end of the decade, terminals evolved into personal computers, while networks went from hierarchical to decentralized, with a broader, generally more numerous collection of servers, and storage scattered throughout an organization. While batch work still existed, many programs became interactive through this age, eventually gaining more advanced visual interfaces along the way. Infrastructure tended to be associated with particular applications and important applications generally demanded enterprise-grade (read: expensive) infrastructure. This period also saw the rise of databases.

Databases were important to business because they held the business data that was manipulated by the applications in the execution of business processes. This data was typically structured, hierarchical, and tightly linked to the associated business processes. Changes in business processes required changes in the underlying database tables and logic. This approach therefore demanded prior knowledge of all aspects of those processes. Business applications were written as tightly coupled interfaces to the data-laden backend, application state found a home in the server, and client-server architectures became central to business.

# Computing Second Age

The second age heralded the rise of the internet—Sun, Cisco, Mosaic (which became Netscape), Web 1.0, eBay, Yahoo, baby.com, and the first internet bubble. It also drove the development and near-ubiquity of easy-to-use, visually attractive devices that could be used by nearly everyone. The biggest technical contribution of the second age was in the network itself. In being forced to deal with the possibility of massive network failures caused by a nuclear attack,

**Notes**

History of Cloud Computing

PPT
**Introduction**

PPT
**Computing First Age**

PPT
**Computing Second Age**

Notes

History of Cloud Computing

PPT

**Computing Third Age**

researchers endowed their invention with the ability to self-organize, to seek out alternate routes for traffic, and to adapt to all sorts of unforeseen circumstances. The single point of failure that was typical of mainframe-inspired networks was removed and in one fell swoop the biggest technological barrier to scaling was eliminated.

Businesses moved quickly in exploiting the new internet, immediately grasping the inherent value of leveraging their tightly coupled client-server applications over the network. As local area networks grew to globally connected wide area networks, network latency and application timeouts made tightly coupled client-server business applications more and more unreliable.

## Computing Third Age

The third age saw the explosion of data and wireless mobility. Email and social media made unstructured data more important than structured data. Early in the second age Yahoo started "indexing the internet," which for some time was mostly manually constructed. While this was sufficient for a while, it soon became apparent that manually built indices could never keep up with the growth of the internet itself. Several other indexing efforts began—including AltaVista, Google, and others—but it was Google where everything came together.

Google realized that the precipitous drop in the cost of storage and rise in the importance of unstructured data had simultaneously reduced the business effectiveness of highly structured databases and associated structured query languages. They revolutionized internet search by automating it with map-reduce, no-SQL, and AppEngine, an early platform-as-a-service. Amazon Web Services innovated business infrastructure though the use of "brutal standardization" and API-driven infrastructure-as-a-service. Salesforce.com rode their Force.com PaaS to becoming the world's first billion-dollar software-as-a-service company. With these business models as proof points, cloud computing was born as an economic model.

Growth of the wireless network, rapid adoption of mobile devices, widespread use of browsers (thin clients) as the business application interface, and the use of virtualization to improve resource utilization made traditionally designed, tightly coupled applications almost useless. Software developers quickly adopted Representational State Transfer (ReST) and created loosely coupled applications where transaction state was moved to the client and no-SQL proved its business value processing unstructured data. With these reverberations, cloud computing was reborn as an operational model.

# Relational Database

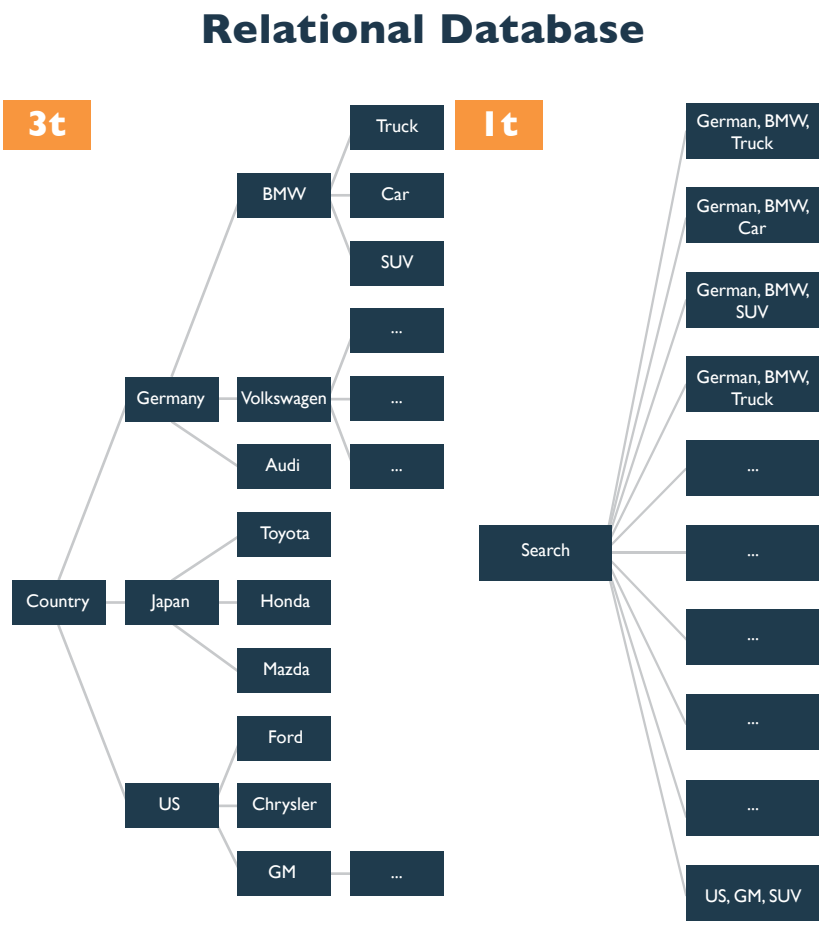



*Figure 1.1: Relational Database*

The economics of data storage led to the use of content-addressable storage, flat storage architectures, and internet scaling. With infinite scalability and consistent responsiveness, database design and database tuning were no longer required.

**Notes**

History of Cloud Computing

**PPT**

**Relational Database**

Notes

History of Cloud Computing

PPT

**Computing Today**

# Computing Today

The development of loosely coupled application architectures and the expansion of elastic and scalable infrastructures led to agile business. These models don't rely on a static business process but exploit parallelism and big data analytics. Executive drive to reduce business costs through the adoption of cloud services has also made infrastructure-centric security models worthless. This is why the enterprise security professional must now adopt a data-centric security model and become a trusted partner with your enterprise business leaders.

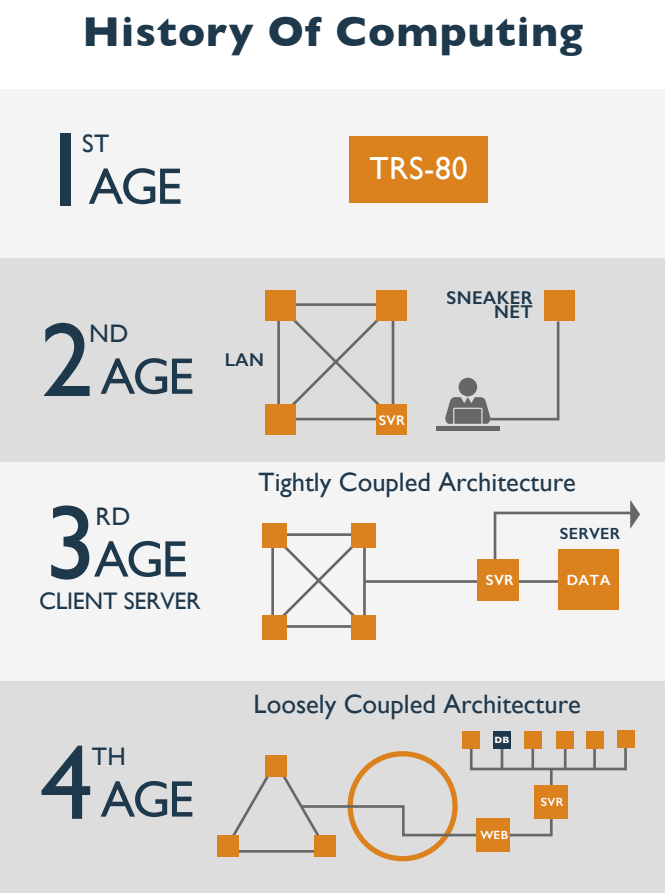



*Figure 1.2: History of Computing*

# Module 2: Understand Cloud Computing Concepts

## Module Topics

- Introduction
- Cloud Computing Definitions
- Key Cloud Computing Characteristics
- Cloud Computing Service Models
- Key Service Advantages
- Cloud Computing Deployment Models
- Implementation Model
- Cloud Computing Strategy
- Cloud Computing Transitions
- Cloud Cross-Cutting Aspects
- Internet Vulnerability and Risks

**Notes**

Understand Cloud Computing Concepts

**PPT**
**Understand Cloud Computing Concepts**

**PPT**
**Module Topics**

**Notes**

Understand Cloud Computing Concepts

**PPT**
**Introduction**

**PPT**
**NIST Definition of Cloud Computing**

# Introduction

Within this module, we will look into the building blocks of all cloud computing solutions. We will provide insights and an overview of cloud concepts, which will include delivery models, service models, provisioning, responsibilities, and functions to which you will become (or already may be) accustomed.

Depending on your role, focus, or cloud resources utilized, these may not all be relevant; however, when communicating and acting from a security perspective, it is imperative to have an understanding and awareness of all the components, services, dependencies, and underlying architecture, infrastructure, and application components in order to address relevant risks, challenges, and threats that may be specific to each layer or service.

**NOTE:** Even if you are an experienced cloud computing practitioner, or someone who is operating within a cloud environment regularly, the following components should be fully understood in order to progress and focus on the future domains.

*"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*

***— N.I.S.T Definition of Cloud Computing***

*http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf*

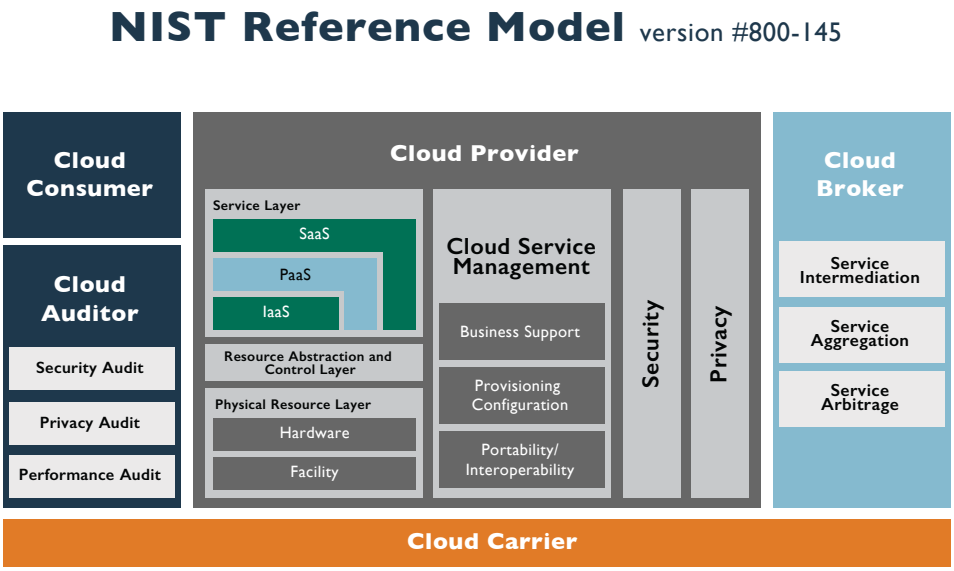



*Figure 1.3: NIST Reference Model*

Cloud computing is the use of internet-based computing resources, typically "as-a-service" to internal or external customers, where scalable and elastic IT-enabled capabilities are provided. There are various definitions of what cloud computing means from NIST, Gartner, and many of the leading standards bodies. The above listed NIST definition is the most commonly and globally utilized, cited by professionals and others alike to clarify what the term "cloud" means.

Cloud computing or "cloud" means many things to many people. As a simple test, simply ask your colleagues at work or your friends what they think of cloud computing, and be prepared for many different answers, interpretations, and viewpoints. Cloud computing is similar to the electricity or power grid: you pay for what you use, it is always on (depending on your geographic location!), and is available to everyone who is connected to the grid (cloud).

The term cloud computing originates from network diagrams/ illustrations where the internet is typically depicted as a "cloud."

In today's information-driven digital economies, the term cloud has been integrated by many organizations, sales personnel, and marketers as a "necessary branding exercise." With Gartner and other leading analyst firms predicting the cloud computing market to be worth over US$200 billion, many traditional IT solution providers are now rebranding themselves as "cloud providers." We will delve into the intricacies of cloud computing over the next few sections, and by the time you complete this course, you will be well positioned to understand the differences between true cloud-based services, managed server-provided models, and traditional enterprise IT services.

"Cloudwashing," adding the word "cloud" in an attempt to rebrand a product, has extended into the very terms used to describe cloud service. "Network-as-a-service," "desktop-as-a-service," "database-as-a-service," "anything-as-a-service," etc., are all used as marketing terms that fundamentally confuse the consumer. Every "as-a-service" offering is basically a component or aggregation of components from the three basic cloud computing services: infrastructure-as-a-service, platform-as-a-service, and software-as-a-service.

A key driver for cloud computing is the shift from capital expenditure (CapEx), where organizations had to invest large sums of money, to operational expenditure (OpEx), which now enables companies to pay per use, and avail themselves of pricing structures similar to monthly or quarterly leasing agreements.

**Notes**

Understand Cloud Computing Concepts

**Notes**

Understand Cloud Computing Concepts

**PPT**

**Key Drivers for Cloud Computing**

Additional drivers include (but are not limited to):

| Term | Definition |
|---|---|
| **Scalability** | Users have access to a large amount of resources that scale based on user demand. |
| **Elasticity** | The environment transparently manages a user's resource utilization based on dynamically changing needs. |
| **Virtualization** | Each user has a single view of the available resources, independent of how they are arranged in terms of physical devices. |
| **Cost** | The pay-per-usage model allows an organization to only pay for the resources they need with basically no investment in the physical resources available in the cloud. There are no infrastructure maintenance or upgrade costs. |
| **Mobility** | Users have the ability to access data and applications from around the globe. |
| **Collaboration** | Users are starting to see the cloud as a way to work simultaneously on common data and information. |
| **Risk reduction** | Users can use the cloud to test ideas and concepts before making major investments in technology. |

### Security/Risks

While many people reference cloud technologies as being "less secure" or carrying greater risk, this is simply not possible or acceptable to say unless making a direct and measured comparison against a specified environment or service.

In truth, the cloud may be more or less secure than your organization's environment and current security controls—this will depend on any number of factors, including the technological components, risk management processes, preventative, detective, and corrective controls, governance and oversight processes, resilience and continuity capabilities, defense in depth, and multiple factor authentication.

As you can see from the list provided, the approach to security will vary depending on the provider and the ability of your organization to alter and amend its overall security posture prior to, during, and after migration or utilization of cloud services.

In the way that no two organizations or entities are alike, the same is true for cloud service providers. A one-size-fits-all approach is never good for security, so do not blindly settle for it when utilizing cloud-based services!

## Cloud Computing Definitions

The following form a key listing of cloud computing definitions and terms that are widely used (some more than others, depending on your industry and geographic location).

**Notes**

Understand Cloud Computing Concepts

**PPT**

**Security/Risks**

**Notes**

Understand Cloud Computing Concepts

| Term | Definition |
|---|---|
| **Anything-as-a-service** | Anything-as-a-service, or "XaaS", refers to the growing diversity of services available over the Internet via cloud computing as opposed to being provided locally, or on-premises. |
| **Apache CloudStack** | An open-source cloud computing and infrastructure-as-a-service (IaaS) platform developed to help make creating, deploying, and managing cloud services easier by providing a complete "stack" of features and components for cloud environments. |
| **Cloud app (cloud application)** | Short for cloud application, cloud app is the phrase used to describe a software application that is never installed on a local computer. Instead, it is accessed via the internet. |
| **Cloud Application Management for Platforms (CAMP)** | A specification designed to ease management of applications—including packaging and deployment—across public and private cloud computing platforms. |
| **Cloud backup** | Cloud backup, or cloud computer backup, refers to backing up data to a remote, cloud-based server. As a form of cloud storage, cloud backup data is stored in and accessible from multiple distributed and connected resources that comprise a cloud. |
| **Cloud backup service provider** | A third-party entity that manages and distributes remote, cloud-based data backup services and solutions to customers from a central data center. |
| **Cloud backup solutions** | Enable enterprises or individuals to store their data and computer files on the internet using a storage service provider, rather than storing the data locally on a physical disk, such as a hard drive or tape backup. |

| Term | Definition |
|---|---|
| **Cloud computing** | A type of computing that relies on sharing computing resources in the delivery of computing services, rather than having local servers or personal devices to handle applications. |
| **Cloud computing accounting software** | Accounting software that is hosted on remote servers. It provides accounting capabilities to businesses in a fashion similar to the SaaS (software-as-a-service) business model. Data is sent into the cloud, where it is processed and returned to the user. All application functions are performed off-site, not on the user's desktop. |
| **Cloud computing reseller** | A company that purchases hosting services from a cloud server or cloud computing provider and then re-sells them to its own customers. |
| **Cloud database** | A database accessible to clients from the cloud and delivered to users on demand via the internet. Also referred to as database-as-a-service (DBaaS), cloud databases can use cloud computing to achieve optimized scaling, high availability, multi-tenancy, and effective resource allocation. |
| **Cloud enablement** | The process of making available one or more of the following services and infrastructures to create a public cloud computing environment: cloud provider, client, and application. |

**Notes**

Understand Cloud Computing Concepts

Notes

Understand Cloud Computing Concepts

| Term | Definition |
|---|---|
| **Cloud management** | Software and technologies designed for operating and monitoring the applications, data, and services residing in the cloud. Cloud management tools help ensure a company's cloud computing–based resources are working optimally and properly interacting with users and other services. |
| **Cloud migration** | The process of transitioning all or part of a company's data, applications, and services from on-site premises behind the firewall to the cloud, where the information can be provided over the internet on an on-demand basis. |
| **Cloud OS** | A software application responsible for orchestrating cloud computing services across multiple, geographically separated data centers. |
| **Cloud portability** | The ability to move applications and their associated data between one cloud provider and another—or between public and private cloud environments. |
| **Cloud provider** | A service provider who offers customers storage or software solutions available via a public network, usually the internet. |
| **Cloud provisioning** | The processes associated with delivering and orchestrating cloud computing services. It also includes facilities for interfacing with the cloud's applications and services as well as auditing and monitoring who accesses and utilizes the resources. |

| Term | Definition |
|---|---|
| **Cloud server hosting** | A type of hosting in which hosting services are made available to customers on demand via the internet. Rather than being provided by a single server or virtual server, cloud server hosting services are provided by multiple connected servers that comprise a cloud. |
| **Cloud storage** | The storage of data online in the cloud, wherein a company's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud. |
| **Cloud testing** | Load and performance testing conducted on the applications and services provided via cloud computing—particularly the capability to access these services—in order to ensure optimal performance and scalability under a wide variety of conditions. |
| **Desktop-as-a-service (DaaS)** | A form of virtual desktop infrastructure (VDI) in which the VDI is outsourced and handled by a third party. Also called hosted desktop services, desktop-as-a-service is frequently delivered as a cloud service along with the apps needed for use on the virtual desktop. |
| **Enterprise application** | Applications—or software—that a business would use to assist the organization in solving enterprise problems. When the word "enterprise" is combined with "application," it usually refers to a software platform that is too large and too complex for individual or small business use. |
| **Enterprise cloud backup** | Enterprise-grade cloud backup solutions typically add essential features such as archiving and disaster recovery to cloud backup solutions. |

**Notes**

Understand Cloud Computing Concepts

Notes

Understand Cloud Computing Concepts

| Term | Definition |
|---|---|
| **Eucalyptus** | An open-source cloud computing and infrastructure-as-a-service (IaaS) platform for enabling private clouds. |
| **Hybrid cloud storage** | A combination of public cloud storage and private cloud storage where some critical data resides in the enterprise's private cloud while other data is stored and accessible from a public cloud storage provider. |
| **Infrastructure-as-a-service (IaaS)** | Computer infrastructure, typically computer, storage and networking services, being delivered as-a-service. IaaS is popular in the data center where software and servers are purchased as a fully outsourced service and usually billed on usage and how much of the resource is used. |
| **Mobile cloud storage** | A form of cloud storage that applies to storing an individual's mobile device data in the cloud and providing the individual with access to the data from anywhere. |
| **Multitenant** | Describes multiple customers using the same public cloud. |
| **Online backup** | Storage technology for backing up data from your hard drive to a remote server or computer using a network connection. Online backup technology leverages the internet and cloud computing to create an attractive off-site storage solution with little hardware requirements for any business of any size. |
| **Personal cloud storage** | A form of cloud storage that applies to storing an individual's data in the cloud and providing the individual with access to the data from anywhere. Personal cloud storage also often enables syncing and sharing stored data across multiple devices such as mobile phones and tablet computers. |

| Term | Definition |
|---|---|
| **Private cloud** | The phrase used to describe a cloud computing platform that is implemented within the corporate firewall, under the control of the IT department. A private cloud is designed to offer the same features and benefits of cloud systems, but removes a number of objections to the cloud computing model, including control over enterprise and customer data, worries about security, and issues connected to regulatory compliance. |
| **Private cloud project** | Companies initiate private cloud projects to enable their IT infrastructure to become more capable of quickly adapting to continually evolving business needs and requirements. Private cloud projects can also be connected to public clouds to create hybrid clouds. |
| **Private cloud security** | A private cloud implementation aims to avoid many of the objections regarding cloud computing security. Because a private cloud setup is implemented safely within the corporate firewall, it remains under the control of the IT department. |
| **Private cloud storage** | A form of cloud storage where the enterprise data and cloud storage resources both reside within the enterprise's data center and behind the firewall. |
| **Public cloud storage** | A form of cloud storage where the enterprise and storage service provider are separate and the data is stored outside of the enterprise's data center. |

**Notes**

Understand Cloud Computing Concepts

Notes

Understand Cloud Computing Concepts

| Term | Definition |
|---|---|
| **Software-as-a-service (SaaS)** | A software delivery method that provides access to software and its functions remotely as a web-based service. SaaS allows organizations to access business functionality at a cost typically less than paying for licensed applications since SaaS pricing is based on a monthly fee. |
| **Storage cloud** | The collection of multiple distributed and connected resources responsible for storing and managing data online in the cloud. |
| **Vertical cloud computing** | A vertical cloud, or vertical cloud computing, describes the optimization of cloud computing and cloud services for a particular vertical (i.e., a specific industry) or specific use application. |

The above form a common list of terms and phrases you will need to become familiar with during your cloud adventures. Variations and evolving terms continue to be utilized outside of the above, but having an understanding of the listed terms will put you in a strong position to communicate and understand technologies, deployments, solutions, and architectures.

# Key Cloud Computing Characteristics

Think of the following as a rule book, or a set of laws when dealing with cloud computing. Where a service or solution does not meet ALL of the following key characteristics, IT IS NOT TRUE CLOUD COMPUTING!

## The Five Essential Characteristics of Cloud Computing

### 1. On-Demand Self-Service

On-demand self-service refers to the cloud service(s) provided that enables the provision of cloud resources on demand (i.e., whenever and wherever they are required). From a security perspective, this has introduced challenges to governing the use and provisioning of cloud-based services, which may violate organizational policies. By its nature, on-demand self-service does not require procurement, provisioning, or approval from finance, and as such can be provisioned by almost anyone with a credit card.

Self-service is also referred to as "self-provisioning," the process where the customer or user is able to provision, manage or operate the cloud services they are utilizing without interaction or assistance from the cloud provider, or cloud provider personnel. It should also be true that all operations and functions should be available for the user to select or configure (based on the cloud service type), through completion of the user or system activities.

### 2. Broad Network Access

Cloud, by its nature, is "always on" and "always accessible" offering users widespread access to resources, data, and other assets. Think convenience! Access what you want, when you need, from any location. Call in and get what you need, when it suits you! In theory, all you should require is internet access and relevant credentials and tokens, which will give you access to the resources. The interesting dynamic of recent times is the mobile device and smart device revolution, which is altering the way organizations fundamentally operate. These devices should be able to access the relevant resources; however, compatibility issues, the inability to apply security controls across all variations, and non-standardization of platforms and software systems has stemmed this somewhat. You may also be aware of "bring your own device" (BYOD), which has ingrained itself into many organizations. We will cover the multiple security, legal, and compliance concerns associated with BYOD in the Legal domain. This allows the user or customer to work

**Notes**

Understand Cloud Computing Concepts

**PPT**

**Key Cloud Computing Characteristics**

Notes

Understand Cloud Computing Concepts

from wherever they need (home, office, on the road), using whichever device they have with them (laptop, smartphone, tablet, desktop, etc.). Ultimately, this is a convenience component, and is a key driver for many cloud users.

### 3. Resource Pooling

Resource pooling lies at the heart of all that is good with cloud computing. Think of the days where if you needed more compute power, you would go to finance, procurement, and embark on a lengthy and often costly process to purchase more computing or compute capability. More often than not, these systems could utilize the resources between 80%–90% for a few hours a week, and reside at an average of 10%–20% for the remainder. The cloud groups (pools) resources for use across the user landscape or multiple clients, which can then be scaled and adjusted to the user's or client's needs based on their workload or resource requirements. Cloud providers typically have large numbers of resources available, from hundreds to thousands of servers, network devices, applications, etc., which can accommodate large volumes of customers, and can prioritize and facilitate appropriate resourcing for each client.

### 4. Rapid Elasticity

Rapid elasticity allows the user to obtain additional resources, storage, compute power, etc., as their need or workload requires. This is most often "transparent" to the user, with more resources added as necessary in a seamless manner. Because cloud services utilize the "pay per use" concept, you only pay for what you use, which is of particular benefit to seasonal or event-type businesses utilizing cloud services. The term plays on the analogy of a large elastic band, which you can pull and stretch depending on the materials that it will hold or secure. Think of a provider selling 100,000 tickets for a major sporting event or concert. Leading up to the ticket release date, little to no compute resources are needed; however, once the tickets go on sale, they may need to accommodate 100,000 users in the space of 30–40 minutes. In this case, rapid elasticity and cloud computing could really be beneficial compared to traditional IT deployments, which would have to invest heavily using capital expenditure (CapEx) to have the ability to support such demand.

### 5. Measured Service

Cloud computing offers this unique and important component, which traditional IT deployments have struggled to provide: resource usage can be measured, controlled, reported, and alerted upon, which results

in multiple benefits and overall transparency between the provider and client. In the same way you may have a metered electricity service, or a mobile phone that you reload with credit, these services allow you to control and be aware of costs. Essentially, you pay for what you use, and have the ability to get an itemized bill or breakdown of usage. A key benefit for many proactive organizations is the ability to charge departments or business units for their use of services, thus allowing IT and finance to quantify exact usage and costs per department or by business function—something that was incredibly difficult to achieve in traditional IT environments.

## Why are these important?

The above listed characteristics enable "true cloud computing," as opposed to grid or traditional hosted computing. In theory and in practice, cloud computing should have large resource pools to enable swift scaling, rapid movement, and flexibility to meet your needs at any given time within the bounds of your service subscription.

Without all of the above characteristics, it is simply not possible for the user to be confident and assured that the delivery and continuity of services will be maintained in line with potential growth or sudden scaling (either upwards or downwards).

One must also internalize the difference between a "cloud service provider" and a "managed service provider." A Managed Service Provider (MSP) will design, implement, and run the acquired service as dictated by and contracted with the enterprise customer. A Cloud Service Provider (CSP) delivers services as designed by the CSP in accordance with an established Service Level Agreement that is typically the same for all the CSP's customers. SLA changes or modifications are negotiated and separately priced. The CSP business model is essentially 180° out from the traditional Request for Proposal (RFP) or MSP acquisition process. A CSP does not create or modify its infrastructure to "meet the customer's requirement." The customer must evaluate CSP SLAs in order to determine if the service will meet its business requirement.

**Multi-tenancy** is a term that you may also see. This refers to a cloud environment where multiple entities (tenants) utilize an architecture in which a single instance serves multiple customers. While tenants may be given the ability to customize some components of the application or service, they cannot customize the relevant code or service for other tenants. With multi-tenancy, each tenant's data is isolated and is not visible or accessible to other tenants. Think of a "one to many" relationship, where users

**Notes**

Understand Cloud Computing Concepts

**PPT**

**Importance of Cloud Computing Characteristics**

Notes

Understand Cloud Computing Concepts

PPT
**Cloud Computing Service Models**

PPT
**Cloud Computing Service Model**

and customers operate alongside each other, separated by controls and "walls" to ensure that no information or data is visible or available to other tenants.

## Cloud Computing Service Models

It's all in the acronym! SaaS, PaaS, and IaaS (SPI) have become synonymous with cloud computing, and when discussing cloud service models, each of these is touted by providers, customers, and sales professionals the world over.

Cloud as we know it today will continue to evolve, with a number of recently coined services and phrases becoming widely used as variations and components of the SaaS, PaaS, and IaaS components. Examples of "XaaS" include storage-as-a-service (SaaS), communications-as-a-service (CaaS), network-as-a-service (NaaS), monitoring-as-a-service (MaaS), and database-as-a-service (DBaaS). The service provider takes responsibility for installing, maintaining, and operating the "XaaS," with the users and customers paying according to their usage. While these terms are often very confusing, it is very important to note that all other "as-a-service" offerings are basically an aggregation or a subset of SaaS, PaaS, or IaaS component.

### Cloud Computing Service Models

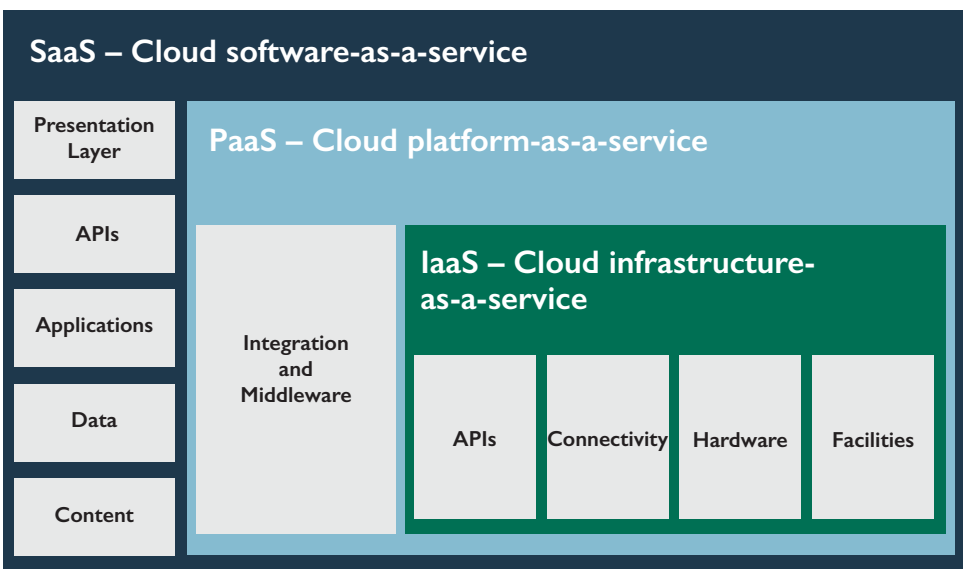



*Figure 1.4: Cloud Computing Service Models*

While the SPI acronym may be catchy, it's best to learn cloud service models from the foundation outward; IaaS through PaaS, and finally SaaS.

## IaaS

Infrastructure-as-a-service (IaaS) is a model where the customer can provision equipment as a service to support operations, including storage, hardware, servers, and relevant networking components. While the consumer has use of the related equipment, the cloud service provider retains ownership, and is ultimately responsible for hosting, running, and maintenance. Infrastructure-as-a-service is also referred to as hardware-as-a-service by some customers and providers.

IaaS has a number of key benefits for organizations, which include, but are not limited to:

- Usage metered and priced on the basis of units (or instances) consumed. This can also be billed back to specific departments or functions.
- Ability to scale infrastructure services up and down based on usage. This is particularly useful and beneficial where there are significant spikes and dips in usage within the infrastructure.
- Reduced cost of ownership. No need to buy assets for everyday use, no loss of asset value over time, and reduction of other related costs of maintenance and support.
- Reduced energy and cooling costs, along with "Green IT" environment effect, with optimum use of IT resources and systems.

## PaaS

Platform-as-a-service (PaaS) is a way for customers to rent hardware, operating systems, storage, and network capacity over the internet from a cloud service provider. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

PaaS has a number of key benefits for developers, which include, but are not limited to:

- Operating systems can be changed and upgraded frequently, including associated features and system services.

**Notes**

Understand Cloud Computing Concepts

PPT
**Infrastructure-as-a-Service (IaaS)**

PPT
**Platform-as-a-Service (PaaS)**

Notes

Understand Cloud Computing Concepts

PPT

**Platform-as-a-Service (PaaS) (continued)**

PPT

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

- Where development teams are scattered globally, or across various geographic locations, the ability to work together on software development projects within the same environment can be extremely beneficial.
- Services are available and can be obtained from diverse sources that cross international boundaries.
- Upfront and recurring or ongoing costs can be significantly reduced by utilizing a single vendor, rather than maintaining multiple hardware facilities and environments.

## SaaS

Software-as-a-service (SaaS) is a distributed model where software applications are hosted by a vendor or cloud service provider and made available to customers over network resources. SaaS is currently the most widely used and adopted form of cloud computing, with users most often simply needing an internet connection and credentials to have full use of the cloud service, application, and data housed.

Within SaaS, there are two delivery models currently used. First, hosted application management (hosted AM), where a cloud provider hosts commercially available software for customers and delivers it over the web (internet). Second, software-on-demand, where a cloud provider provides customers with network-based access to a single copy of an application created specifically for SaaS distribution (typically within the same network segment).

Software-as-a-service has a number of key benefits for organizations, which include, but are not limited to:

- Ease of use and limited/minimal administration.
- Automatic updates and patch management; always running the latest version and most up-to-date deployment (no manual updates required).
- Standardization and compatibility (all users have the same version of software).
- Globally accessibility.

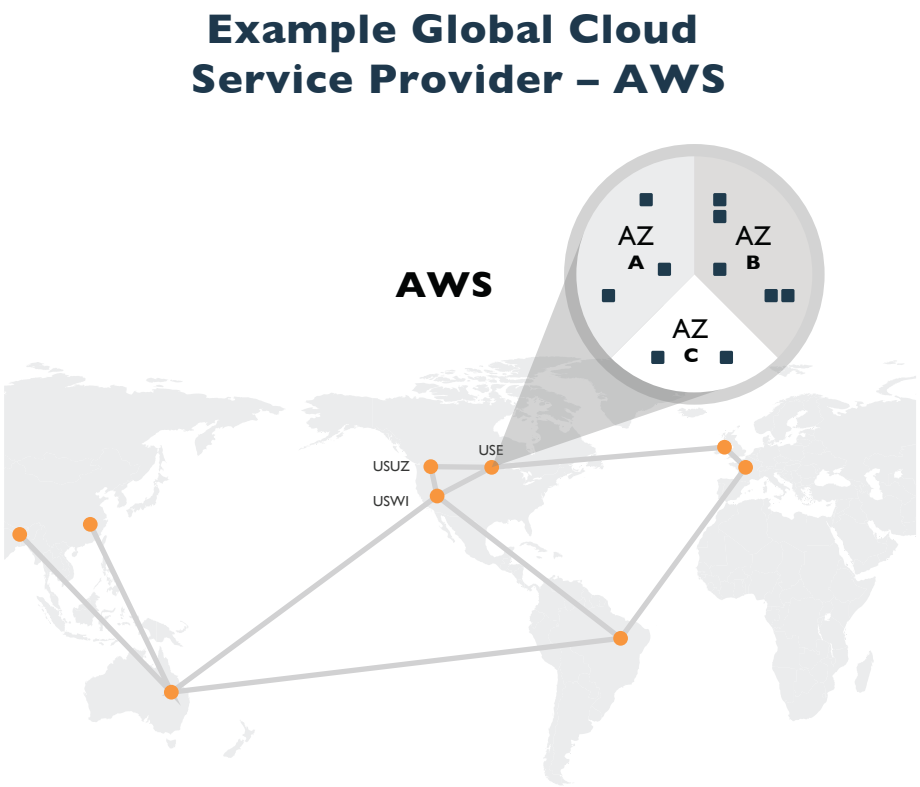



*Figure 1.5: Example Global Cloud Service Provider – AWS*

***Resource:*** *https://aws.amazon.com/about-aws/global-infrastructure/*

# Key Service Advantages

## Software Application

Cloud computing provides significant and potentially limitless possibilities for organizations to run programs and applications which may previously have not been practical or feasible given the limitations of their own systems, infrastructure, or resources.

When utilizing and deploying the right middleware and associated components, the ability to run and execute programs with flexibility, scalability, and on-demand self-service capabilities can present massive incentives and benefits.

Clients are able to access their applications and data from anywhere, at any time. They can access the cloud computing system using any computer linked to the internet. Data aren't confined to a hard drive on one user's computer or even a corporation's internal network. Other capabilities and benefits include:

**Notes**

Understand Cloud Computing Concepts

**PPT**

**Key Service Advantages**

Notes

Understand Cloud Computing Concepts

PPT

**Key Service Advantages (continued)**

- **Overall reduction of costs:** Cloud deployments reduce the need for advanced hardware on the client side. Essentially, the requirement to purchase high specification systems, redundancy, storage etc. to support the applications is no longer necessary. From a customer perspective, a device to connect to the relevant application with the appropriate middleware is all that should be required.
- **Application and software licensing:** Customers no longer need to purchase licenses, support, and associated costs, as licensing is "leased" and is relevant only when in use (covered by the provider). Additionally, purchasing of bulk licensing and the associated CapEx is removed and replaced by a pay-per-use licensing model.
- **Reduced support costs:** Customers save money on support issues, as these are handled by the relevant cloud provider. Appropriately managed, owned and operated streamlined hardware would, in theory, have fewer problems than a network of heterogeneous machines and operating systems.
- **Backend systems and capabilities:** Where applications back onto grid and cloud environments, this provides the ability to pull processing and compute power to assist with resource intensive tasks.

## Platform

PaaS and the cloud platform components have revolutionized the manner in which development and software has been delivered to customers and users over the past few years. The barrier for entry in terms of costs, resources, capabilities, and ease of use have dramatically reduced "time to market," promoting and harvesting the innovative culture within many organizations.

Outside of the key benefits, platform should have the following key capabilities and characteristics:

- **Support multiple languages and frameworks:** Platform should support multiple programming languages and frameworks, thus enabling the developers to code in whichever language they prefer or the design requirements specify. In recent times, significant strides have been made and efforts have been taken to ensure that open-source stacks are both supported and utilized, thus reducing "lock in" or issues with interoperability when changing cloud providers.
- **Multiple hosted environments:** The ability to support a wide variety of underlying hosting environments for the platform is key to meeting customer requirements and demands. Whether public

cloud, private cloud, local hypervisor, or bare metal, supporting multiple hosting environments allows the application developer or administrator to migrate their application when and as required. This can also be used as a form of contingency and continuity, and to ensure ongoing availability.

- **Flexibility:** Traditionally, platform providers provided features and requirements that they felt suited the client requirements, suited their service offering, and positioned them as the provider of choice, with limited options for the customers to move easily. This has changed drastically, with extensibility and flexibility now afforded to meeting the developer requirements. This has been heavily influenced by open source, which allows relevant plugins to the platform.
- **Allow choice and reduce "lock-in":** "Proprietary" usually means red tape, barriers, and restrictions on what developers can do when it comes to migration or adding features and components to the platform. With the requirement to code to specific APIs made available by the provider, you can now run your apps in various environments, based on commonality and standard API structures, ensuring a level of consistency and quality for customers and users.
- **Ability to "auto-scale":** Probably one of the biggest drivers, this enables the application to seamlessly scale and accommodate the demand of users. The platform will allocate resources and assign them to the application as required. This serves as a key driver for organizations that experience spikes and drops in usage (e.g., seasonal sales).

## Infrastructure

Since the dawn of computing, infrastructure has been the focal component to ensuring which capabilities and organizational requirements could be met, versus those that were restricted. It also represented possibly the most significant investments in terms of CapEx and skilled resources. Because infrastructure served as a key and core component for IT teams and technology professionals around the world, it became a significant cost base and expense when delivering and providing the relevant services to the organization.

**Notes**

Understand Cloud Computing Concepts

**PPT**

**Key Service Advantages (continued)**

Notes

Understand Cloud Computing Concepts

PPT
**Cloud Service Derivatives**

PPT
**Cloud Computing Deployment Models**

Within the cloud, this has changed significantly. However, the following key components and characteristics remain in order to meet and achieve the relevant requirements:

- **Scale:** Automation and tools to support the potentially significant workloads of either internal users or those across multiple cloud deployments (dependent on the cloud service offering) are key components of infrastructure. Users and customers require optimal levels of visibility, control, and assurances related to the infrastructure and its ability to satisfy their requirements.
- **Converged network and IT capacity pool:** Building on the scale component, this looks to drill into the virtualization and service management components required to cover and provide appropriate levels of service across network boundaries. From a customer or user perspective, the pool appears seamless and endless (no visible barriers or restrictions, along with minimal requirement to initiate additional resources) for both servers and networks. These should be at all times focused on supporting and meeting relevant platforms, applications, and SLAs.
- **Self-service and on-demand capacity:** Requires an online resource or customer portal that allows customers to have complete visibility and awareness of the virtual IaaS environment that they currently utilize. Additionally, this should also allow customers to acquire, remove, manage, and report on resources, without the need to engage or speak with internal resources or with the provider. Think online banking—the same ease of use, without having to go to the branch.
- **High reliability and resilience:** In order to be effective, there must be automated distribution across the virtualized infrastructure (LAN and WAN), increasing and affording resilience, while enforcing and meeting SLA requirements.

## Cloud Computing Deployment Models

Now that you are equipped with an understanding and appreciation of the cloud service types, we will look to understand how these services are merged into the relevant deployment models. The selection of a cloud deployment model will depend on any number of factors, and may well be heavily influenced by your organization's risk appetite; cost, compliance, and regulatory requirements; legal obligations; and other internal business decisions and strategy.

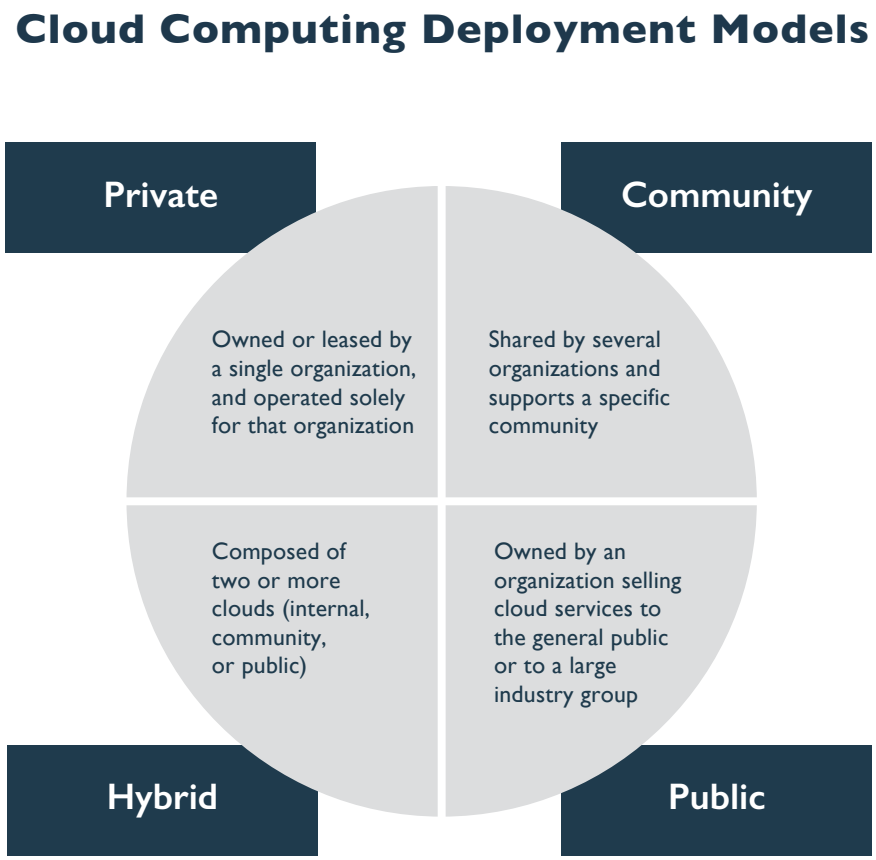



*Figure 1.6: Cloud Computing Deployment Models*

## Public

A public cloud is the service available to the general public over the internet, in which a customer can access cloud service provider resources, such as applications and storage, on demand, either in the form of a free service or offered on a pay-per-usage model.

Key drivers or benefits of public cloud typically include:

- Easy and inexpensive set-up because hardware, application, and bandwidth costs are covered by the provider.
- Streamlined provisioning of resources.
- Scalability to meet customer needs.
- No wasted resources (pay per usage).

Given the increasing demands for public cloud services, many providers are now offering and remodeling their services as public cloud offerings. Significant and notable providers in the public cloud space include Amazon, Microsoft, Salesforce, and Google Apps, among others.

**Notes**

Understand Cloud Computing Concepts

**PPT**

**Cloud Computing Deployment Models (continued)**

**PPT**

**Public Cloud**

Notes

Understand Cloud Computing Concepts

PPT
**Private Cloud**

PPT
**Hybrid Cloud**

## Private

A private cloud service refers to a proprietary network, or data center, owned and architected for use by a specified entity utilizing cloud technologies to provide services behind a firewall. A private cloud is typically managed by the organization it serves; however, a recent increase in outsourcing the general management of this to trusted third parties has been noted. A private cloud is typically only available to the entity or organization, its employees, contractors, and selected third parties.

The private cloud is also sometimes referred to as the "internal" or "organizational cloud."

Key drivers or benefits of private cloud typically include:

- Increased control over data, underlying systems, and applications.
- Ownership and retention of governance controls.
- Assurance over data location.

Private clouds are typically more popular among large, complex organizations with legacy systems and heavily customized environments. Additionally, where a significant technology investment has been made, it may be more financially viable to utilize and incorporate these investments within a private cloud environment than to discard or retire such devices.

## Hybrid

A hybrid cloud is built by combining multiple forms of cloud computing deployment models, typically public and private cloud. Hybrid cloud computing is gaining in popularity, as it provides organizations the ability to retain control of their IT environments, offers the convenience of allowing organizations to use public cloud service to fulfill non-mission-critical workloads, and takes advantage of flexibility, scalability, and cost savings.

Key drivers or benefits of hybrid cloud deployments include:

- Retain ownership and oversight of critical tasks and processes related to technology.
- Reuse previous investments in technology within the organization.
- Control over most critical business components and systems.
- Cost-effective means of fulfilling non-critical business functions (utilizing public cloud components).
- "Cloud bursting" (when your private cloud workload maximum is reached, utilizes public cloud resources to help support) and disaster recovery can be enhanced by hybrid cloud deployments.

**NOTE:** While numerous benefits are realized with hybrid cloud deployments and cloud models, these can often be time consuming and laborious at the start, as most companies and entities encounter integration and migration issues along with other issues at the outset.

### Community

Community clouds are not as widely utilized as the public, private, or hybrid deployment models. They can, however, offer a valuable and cost-effective manner for specified groups or entities with a similar focus, or with common compliance and requirements, to operate in a multi-tenant infrastructure. Community clouds can be on-premises or off-site, and should give the benefits of a public cloud deployment, while providing heightened levels of privacy, security, and regulatory compliance.

## Implementation Model

Cloud computing is never the only information technology deployment option. Enterprises also have at least three implementation strategy options:

- Continue a status quo strategy that uses a traditional enterprise data center to address requirements.
- Select and contract with a Managed Service Provider (MSP) by running a traditional acquisition that dictates requirements and operational processes through the RFP/Bid process.
- Satisfy requirements through the use of standard offerings from one or more Cloud Service Provider (CSP).

The primary drivers in an implementation model selection is enforcement of enterprise IT governance processes (status quo and MSP option) or acceptance of CSP IT governance processes (CSP option).

## Cloud Computing Strategy

When developing an enterprise cloud computing strategy, there are theoretically 36 point solutions that should be investigated (4[Deployment Models] x 3[Service Models] x 3[Implementation options]=36 Point Solutions). Real world deployments are typically a blend of multiple theoretical point solutions. The model is, however, useful in comparing options and designing target architectures.

**Notes**

Understand Cloud Computing Concepts

PPT
**Community Cloud**

PPT
**Implementation Model**

PPT
**Cloud Computing Strategy Options**

**Notes**

Understand Cloud Computing Concepts

**PPT**
**Cloud Computing Transitions**

**PPT**
**Cloud Cross-Cutting Aspects**

# Cloud Computing Transitions

When undertaking any transition to cloud computing, organizations must also consider the effect on existing information technology governance and/or policies that spread over multiple operational domains. Relevant operational domains and transition vectors are summarized in Table 1.1.

### Cloud Strategy Operational Domains and Transition Vectors

| Domain | Transition From | Transition To |
|---|---|---|
| **Security Framework** | Infrastructure-Centric | Data-Centric |
| **Application Development** | Tightly Coupled | Loosely Coupled |
| **Data** | Mostly Structured | Mostly Unstructured |
| **Business Processes** | Mostly Serial | Mostly Parallel |
| **Security Controls** | Enterprise Responsibility | Share Responsibility |
| **Economic Model** | Mostly CapEx | Mostly OpEx |
| **Infrastructure** | Mostly Physical | Mostly Virtual |
| **IT Operations** | Mostly Manual | Mostly Automated |
| **Operational Scope** | Local/Regional | International/Global |

*Table 1.1: Cloud Strategy Operational Domains and Transition Vectors*

# Cloud Cross-Cutting Aspects

The cloud, by its nature, is often deemed a technology decision. While cloud computing no doubt enables technology to be delivered and utilized in a unique manner, potentially unleashing multiple benefits, this should be a business decision, taken in line with the business's or organization's overall strategy.

Why a business decision? Two distinct reasons: first, all technology decisions should be made with the overall business direction and strategy at the core; and second, when it comes to funding and creating opportunities, these decisions should be made at a business level. At times, we as technology professionals are guilty of "tech speak"—we consistently revert to talking about technology at the "nuts and bolts level," when all business executives and senior decisions makers are concerned about is "Why does the business need this?"

While the cloud can certainly provide benefits to your organization in some way, shape, or form, the ability to craft and interpret that message in a business manner, outlining what the return on investment (not always financial!) will be might just be the difference between a successful project versus a failed or declined project.

## Interoperability

Interoperability is the requirement for the components of a cloud eco-systems to work together to achieve their intended result. In a cloud computing eco-system, the components may well come from different sources, both cloud and traditional, both public and private cloud implementation (known as hybrid-cloud). Interoperability mandates that those components should be replaceable by new or different components from different providers and continue to work, as should the exchange of data between systems.

In summary, if your car engine fails, you should be able to replace the engine with the same brand or type of engine, or alternatively look for another engine that will provide the same level of power and function to the car to allow it to continue to operate. Interoperability uses the same premise: continued availability of services, regardless of providers or cloud components.

## Portability

Portability defines the ease with which application components are moved and reused elsewhere regardless of the provider, platform, OS, infrastructure, location, storage, format of data, or APIs. Portability is a key aspect to consider when selecting cloud providers, since it can both help prevent vendor lock-in and deliver business benefits by allowing identical cloud deployments to occur in different cloud provider solutions, either for the purposes of disaster recovery or for the global deployment of a distributed single solution.

Again, think of car components. Light bulbs, brakes, and other standard components could be switched out, yet would still continue to function.

## Availability

Systems and resource availability defines the success or failure of a cloud-based service. Availability is a single point of failure for cloud-based services. If the service or cloud deployment loses availability,

**Notes**

Understand Cloud Computing Concepts

**PPT**

**Cloud Cross-Cutting Aspects (continued)**

Notes

Understand Cloud Computing Concepts

PPT

**Cloud Cross-Cutting Aspects (continued)**

the customer is unable to access their target assets or resources, resulting in downtime. In many cases, cloud providers are required to provide upwards of 99% availability as per the service-level agreement. Failure to do so can result in penalties, reimbursement of fees, loss of customers, loss of confidence, and ultimately, brand and reputational damage.

## Security

For many customers and potential cloud users, security remains the single biggest concern, with as many as 60% of business users stating that security concerns are the number one restriction or barrier preventing them from engaging with cloud services. As with any successful security program, the ability to measure, obtain assurance, and integrate contractual obligations to minimum levels of security are key. Many cloud providers now list their typical or minimum levels of security, but will not list or publicly state specific security controls (for fear of their infrastructures being targeted by attack vectors and threats). When contracts and engagements require specific security controls and techniques to be applied, these are typically seen as "extras" that will incur additional costs and require the relevant non-disclosure agreements (NDAs) to be completed before engaging in active discussions.

In many cases, for smaller organizations, a move to cloud-based services will significantly enhance their security controls, given that they may not have access to or possess the relevant security capabilities of a large-scale cloud-computing provider.

The general rule of thumb for security controls and requirements in cloud-based environments is "If you want additional security, additional cost will be incurred." You can have whatever you want when it comes to cloud security—just as long you as you can find the right provider and you are willing to pay for it!

## Privacy

In the world of cloud computing, privacy presents a major challenge for both customers and providers alike. The reason for this is simple: no uniform or international privacy directives, laws, regulations or controls exist, leading to a separate, disparate, and segmented mesh of laws and regulations being applicable, depending on the geographic location where the information may reside (data at rest) or be transmitted (data in transit). Given the true global nature and various international locations of cloud-computing data centers, this could mean that your organization's data could reside in two, three, or more locations around the world at any given time. For many European entities and organizations, this violates EU Data Protection laws and obligations, which could lead to various issues

and implications. Within Europe, privacy is seen as a human right, and as such should be treated with the utmost respect. Not bypassing the various state laws across the United States and other geographic locations requires an extremely complex and intricate level of knowledge and controls to ensure that no such violations or breaches of privacy and data protection occur.

## Resiliency

Cloud resiliency represents the ability of a cloud services data center and its associated components, including servers, storage, etc., to continue operating in the event of a disruption, which may be equipment failure, power outage, or a natural disaster. In summary, resilience represents the ability to continue service and business operations in the event of a disruption or event. Given that most cloud providers have a significantly higher number of devices and redundancy in place than a standard "in-house" IT team, resiliency should typically be far higher, with equipment and capabilities ready to failover, multiple layers of redundancy, and enhanced exercises to test such capabilities.

## Performance

Cloud computing and high performance should go hand in hand at all times. Let's face it—if the performance is poor, you may not be a customer for very long. For optimum performance to be experienced throughout the use of cloud services, the provisioning, elasticity, and other associated components should always focus on performance. If you wish to travel by boat, the speed at which you can travel is dependent on the engine and the boat design. The same applies for performance, which at all times should be focused on the network, the compute, the storage, and the data. With these four elements influencing the design, integration, and development activities, performance should be boosted and enhanced throughout. Remember, it is always harder to refine and amend performance once design and development have been completed.

## Governance

The term "governance," when relating to processes and decisions, refers to defining actions, assigning responsibilities, and verifying performance. The same can be said and adopted for cloud services and environments where the goal is to secure applications and data when in transit and at rest. In many cases, cloud governance is an extension of existing organizational or traditional business process governance, with a slightly altered risk and controls landscape. While

**Notes**

Understand Cloud Computing Concepts

**PPT**

**Cloud Cross-Cutting Aspects (continued)**

Notes

Understand Cloud Computing Concepts

PPT

**Cloud Cross-Cutting Aspects (continued)**

governance is required from the commencement of a cloud strategy or cloud migration roadmap, it is seen as a recurring activity and should be performed on an ongoing basis. A key benefit of many cloud-based services is the ability to access relevant reporting, metrics, and up-to-date statistics related to usage, actions, activities, downtime, outages, updates, etc. This may enhance and streamline the governance and oversight activities with the addition of scheduled and automated reporting available.

**NOTE:** Processes, procedures, and activities may require revision after migration or movement to a cloud-based environment. Not all processes remain the same. Segregation of duties, reporting, and incident management are examples of processes that may require revision after cloud migration.

## Service-Level Agreements (SLAs)

Think of a rule book and legal contract—that combination is what you have in an SLA. Some go so far as to call it the prenup (prenuptial agreement between yourself and your provider). Let us not underestimate or downplay the importance of this document/agreement. In it, the minimum level of service, availability, security, controls, processes, communications, support, and many other crucial business elements are stated and agreed to by both parties.

Many may argue that the SLAs are heavily weighted in favor of the cloud service provider, but there are a number of key benefits when compared with traditional environments or "in-house IT." These include downtime, upgrades, updates, patching, vulnerability testing, application coding, test and development, support, and release management. Many of these force the provider to take these areas and activities very seriously, as failing to do so will impact their bottom line.

**NOTE:** Not all SLAs cover the areas or focus points you may have issues or concerns with. Where this is not the case, every effort should be made to obtain clarity prior to engaging with the cloud service provider. If you think it is time-consuming moving to cloud environments, wait until you try to get out!

## Auditability

Auditability relies on a single key component: evidence. Think of the auditor coming in with their checklist and questions—that is the same mindset that your organization or entity should take to ensure that you at all times have a comfort with and positive understanding of your ability to audit and measure actions against requirements. Systems and processes will fail, so wherever possible, auditing and auditability should provide sufficient information, details, and evidence to support reviews and investigations.

The ability to point to audit results, findings, and relevant evidence has not only saved jobs and companies from catastrophic impacts, but has also given leaders the facts and reports they need to alter business processes, system functions, and personnel activities and to implement increased safeguards such as defense in depth or additional layers of security and risk management.

### Regulatory

Regulatory compliance (also known as regcompliance) is an organization's requirement to adhere to relevant laws, regulations, guidelines, and specifications relevant to its business, specifically dictated by the nature of operations and functions it provides to its customers. Where the organization fails to meet, or violates, regulatory compliance regulations, punishment can include legal actions, fines, and in limited cases, halting business operations or practices.

Key areas that are often included in cloud-based environments include (but are not limited to), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA), and the Sarbanes–Oxley Act (SOX).

## Internet Vulnerability and Risks

Media coverage seems to imply that large-scale data breaches, hacks, and online financial crime are rampant. Reports from information technology security firms like Norton Symantec and Kaspersky Labs also generally show the security of cyberspace as poor and often getting worse. This is one reason why the Global Commission on Internet Governance was formed in January, 2014. Launched by two independent global think tanks, the Centre for International Governance Innovation (CIGI) and Chatham House, the Global Commission on Internet Governance was designed to help educate the wider public on the most effective ways to promote internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas. This two-year project conducted independent research on internet-related dimensions of global public policy, culminating in an official commission report that articulated concrete policy recommendations for the future of internet governance. These recommendations addressed concerns about the stability, interoperability, security, and resilience of the internet ecosystem.

**Notes**

Understand Cloud Computing Concepts

PPT
**Cloud Cross-Cutting Aspects (continued)**

PPT
**Application Development Process**

PPT
**Internet Vulnerability and Risks**

Notes

Understand Cloud Computing Concepts

PPT

**Internet Vulnerability and Risks (continued)**

In the executive summary, the final report argued that the level of security in cyberspace is actually far better than the picture described by media accounts and IT security reports. In these reports, numbers on the occurrence of cybercrime are usually depicted in either absolute (1,000 attacks per year) or as year-over-year percentage change terms (50 percent more attacks in 2014 than in 2013). To get a more accurate picture of the security of cyberspace, the Commission expressed these statistics as a proportion of the growing size of the internet (similar to the routine practice of expressing crime as a proportion of a population, e.g., 15 murders per 1,000 people per year). This data was then collected on the vectors of cyberattack, the occurrence of cyberattacks, and the cost of cybercrime.

Normalizing these crime statistics around various measures of the growing size of cyberspace, a clearer picture emerges: the absolute numbers always paint a worse scenario of the security of cyberspace than the normalized numbers. Absolute numbers tend to lead to one of three misrepresentations: first, the absolute numbers say things are getting worse, while the normalized numbers show that the situation is improving; second, both numbers show that things are improving, but the normalized numbers show that things are getting better at a faster rate; and third, both numbers say that things are getting worse, but the normalized numbers indicate that the situation is deteriorating more slowly than the absolute numbers. Overall, global cyberspace is actually far safer than commonly thought. Security professionals should keep these thoughts in mind when discussing this subject with colleagues.

When it comes to the costs of cybercrime, the internet's value added is currently outpacing the costs that internet-enabled cybercrime imposes on society. In net terms, having the internet is still beneficial, even though cybercrime inflicts economic damage. In fact, the average financial cost of a single data breach could exceed $12M per $1B of internet-based revenue. This financial loss consists of:

- Organizational costs: $6,233,941
- Detection and escalation costs: $372,272
- Response costs: $1,511,804
- Lost business costs: $3,827,732
- Victim notification cost: $523,965

At a social level, what matters are net gains, and, in the case of the internet and cybercrime, this 1.2% financial leakage is not too bad. From a security professional's point of view, however, the business case for a significant investment in operational security to avoid a breach looks even better!

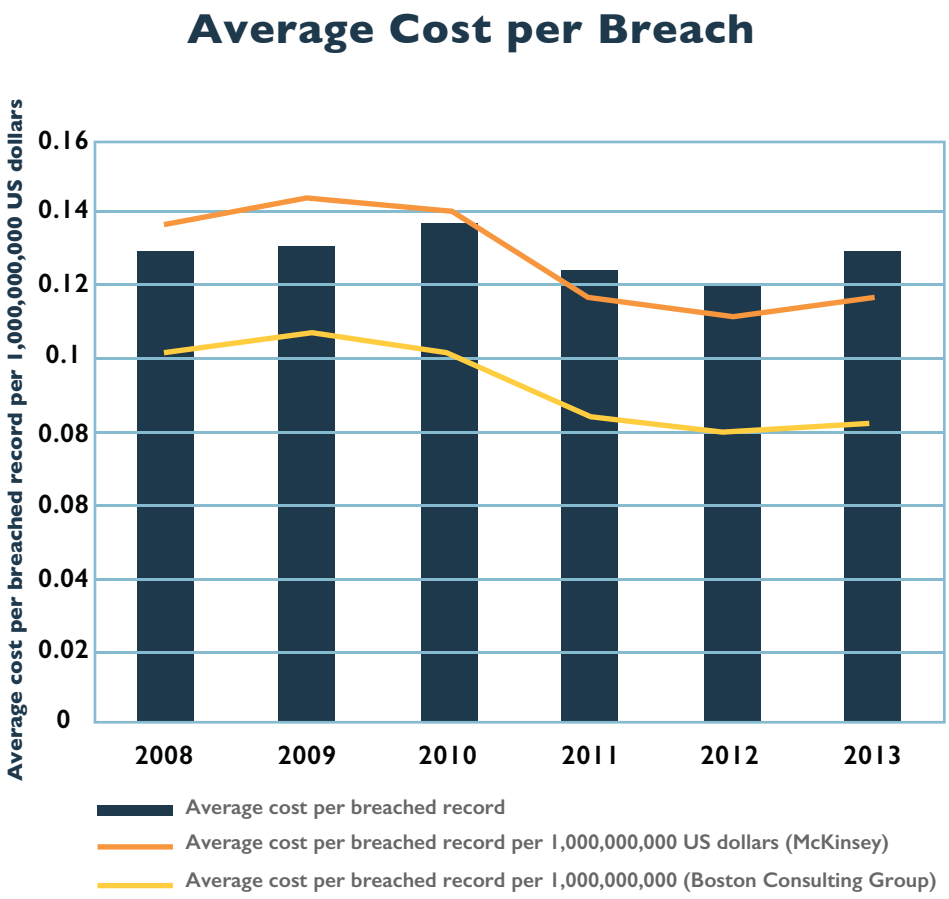



*Figure 1.7: Average Cost per Breach*

**Notes**

Understand Cloud Computing Concepts

**PPT**

**Average Cost per Breach**

Notes

Cloud Economic Model

PPT
Cloud Economic Model

PPT
Module Topics

# Module 3: Cloud Economic Model

## Module Topics

- Introduction
- Economic Impact of the Cloud-Computing Model
- Enterprise IT versus Managed Service Provider versus Cloud Service Provider
- Economic Impact of the IT Service Delivery Model
- Private Cloud Transition Economics
- Public Cloud Adoption Economics
- Cloud Computing Return on Investment
- Acquisition and Governance Changes

# Introduction

NIST defines cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. NIST implies the economy of scale that goes with cloud computing when they talk about a pool of configurable computing resources.

Cloud computing is often referred to as a technology. However, it is actually a paradigm shift in the business and economic models for provisioning and consuming information technology that can lead to a significant cost savings. This cost savings can only be realized through the use of significant pooling of these "configurable computing resources" or resource pooling. According to NIST, this capability is an **essential characteristic** of cloud computing. Resource pooling defines the ability of a cloud to serve multiple consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Cloud computing economics depends on four customer population metrics:

- Number of unique customer sets (n)
- Customer set duty cycles (λ,f)
- Relative duty cycle displacement (t)
- Customer set load (L)

These factors drive the cloud provider's ability to use the minimum amount of physical IT resources to service a maximum level of IT resource demand. Properly balancing these factors across a well-characterized user group can lead to ~30% savings in IT resources. This enables the near-real-time modification of the underlying physical infrastructure required for the delivery of the desired "illusion of infinite resources" that is synonymous with a cloud computing user's experience.

**Notes**

Cloud Economic Model

**PPT**

**Introduction**

Notes

Cloud Economic Model

PPT

**Economic Impact of the Cloud Computing Model**

# Economic Impact of the Cloud Computing Model

Cloud service providers bring massive economies of scale to computing and delivers computing resources on demand. Before cloud computing, companies had to make ever-growing capital expenditures (CapEx) in computing resources to implement new information systems, and to accommodate potential peak loads. This led to overcapacity and underutilization. Cloud computing is a variable operation expenditure (OpEx) model. This can eliminate long-term investments when exploring new business models or help exploit short-term business opportunities.

This is because cloud computing services are consumed using a variable (OpEx) model, which:

1. Eliminates long term investments when exploring new business models.
2. Is an efficient enabler of cross-device access and synchronization of content or applications across a single user with multiple devices.
3. Eliminates hardware costs normally associated with new systems or services.

This combination drives the information technology industry away from highly customized independent architectures, which generally drive prevailing prices upward. Cloud computing drives the industry towards pooled resources, shared architectures, flat-rate pricing models and pay-per-use pricing models, which generally lowers prevailing prices.

# Enterprise IT versus Managed Service Provider versus Cloud Service Provider

Traditionally, the enterprise management will develop and impose IT governance. IT management will generally monitor and report on organizational adherence, changing and modifying the IT infrastructure as needed or directed. IT procurement and operational expenditures are also managed via IT governance processes. Acquisition requirements are delineated using the traditional request for proposal (RFP) or request for quote (RFQ), and vendor selection is driven by vendor compliance with the specified requirements and a negotiated price.

When enterprises opt to use managed service providers for information technology, compliance with enterprise-imposed IT governance is typically required. The cost of delivering a compliant solution is generally recouped by the provider during a mutually agreed minimum service period.

Cloud service providers fund and build their infrastructure based on the forecasted requirements of an IT marketplace segment and a forecasted penetration into that market, not a specific marketplace customer. Services offering line sheet and pricing models are set based on CSP investment, marketplace uptake of their service offerings, and realized CSP profit. IT governance is typically a shared model within which CSP responsibilities are generally fixed and consistent across all CSP customers. Any enterprise consuming CSP services must conduct sufficient due diligence in order to:

- Clearly understand CSP responsibilities, enterprise responsibilities, and demarcation between the two.
- Ensure that CSP IT governance processes and procedures are compatible with those of the enterprise and its operating environment.
- Ensure that operating on the CSP infrastructure is compliant with any legal, regulatory, or industry requirements.
- Ensure that the enterprise has sufficient operational visibility and documentation to meet all audit and security requirements.

**Notes**

Cloud Economic Model

**PPT**

**Enterprise IT versus Managed Service Provider versus Cloud Service Provider**

Notes

Cloud Economic Model

PPT

**Economic Impact of the IT Service Delivery Model**

# Economic Impact of the IT Service Delivery Model

A 2009 Booz Allen Hamilton study concluded that a cloud computing approach could save from 50%–67% on the lifecycle cost for a 1,000-server deployment. A separate Deloitte study confirmed that cloud computing deployments delivered greater investment returns with a shorter payback period when compared to the traditional on-premises option. These studies prove that when implemented properly, the IT service delivery model can drastically reduce the operations and maintenance cost of IT infrastructures.

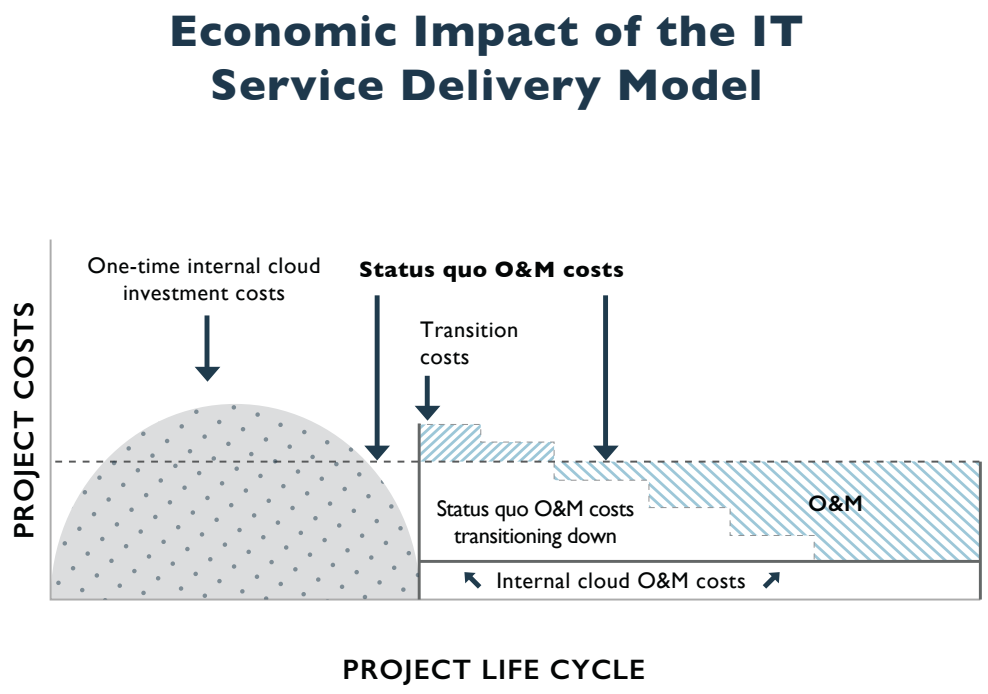



*Figure 1.8: Economic Impact of the IT Service Delivery Model*

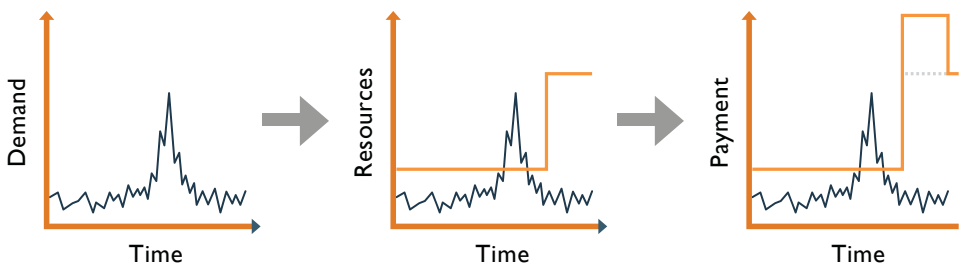
## Economic Impact of the Cloud-Computing Model

Businesses must always deal with the disparity between the capacity to produce products and deliver services—which is fixed in the short term—and the demand for those products and service—which is almost always variable at any time scale. Customer demand in just about any circumstance is volatile. While some tactical measures can be taken to alleviate some scenarios, cloud-computing models have been shown capable of economically solving the so-called "demand dilemma" when applied to cloud computing–compatible business models.

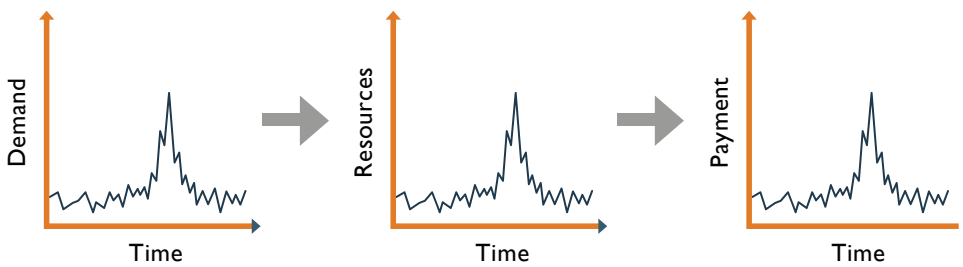
Cloud computing can economically address the "Capacity Conundrum" where companies build capacity to match peak demand, which typically

leads to substantial excess capacity during off-peak periods. This excess capacity represents either nonproductive capital or unnecessary expense. Conversely, if capacity is sized to the baseline, there will be insufficient resources to handle spikes. Transactions not served represent demand for the products or services that the business would have monetized, resulting in lost revenue or lost worker productivity.

**Traditional versus Cloud Model**




**(a) Traditional Model (CapEx)**




**(b) On Demand, Pay per Use (OpEx)**

*Figure 1.9: Traditional versus Cloud Model*

## Private Cloud Transition Economics

Transitioning from a traditional enterprise IT infrastructure to the private cloud model involves a significant level of investment, operational modifications, and cultural change. Investment is driven by an increased use of automation, staff skillset enhancements, and training costs associated with needed operational changes.

Operational modifications are associated mostly with "brutal" enforcement of standards across the organization. Aggressive enforcement of standards is essential to the broad and deep deployment of automation needed to effect significant staff reductions and effective service level management.

**Notes**

Cloud Economic Model

**PPT**
**Economic Impact of the IT Service Delivery Model (continued)**

**PPT**
**Traditional Versus Cloud Model**

**PPT**
**Private Cloud Transition Economics**

**Notes**

Cloud Economic Model

**PPT**
**Private Cloud Transition Economics (continued)**

**PPT**
**Public Cloud Adoption Economics**

**PPT**
**Public Cloud Service Provider ROI Model**

The significant cultural changes associated with the aforementioned operational modifications should not be underestimated. Cultural changes will permeate the entire organization for five or more years if done across a global organization. Research has also shown that the cost of private cloud deployments may exceed the operating cost of an established traditional operation. Organizations should also be cautioned about the relative rarity of cost savings being associated with a transition to a private cloud. Cost savings are much more likely if a subset of requirements are addressed through a private cloud and the balance appropriately met with the adoption of public or community cloud services. Resulting hybrid cloud models have been shown to significantly reduce operating cost while simultaneously improving operational efficiency.

## Public Cloud Adoption Economics

Public cloud adoption has historically delivered significant enterprise IT cost savings through significantly reduced capital expenditures, staff level reductions, and increased operational efficiencies. These well-documented results are driven primarily by the public cloud service provider's ability to deliver a continuously improving level of service at lower cost and higher profit margins. Consistency in these trends are reinforced by global scale, very low marginal cost to deliver services to additional customers, and steadily improving CSP operational efficiencies. A public cloud service provider ROI model example is shown in Figure 1.10.

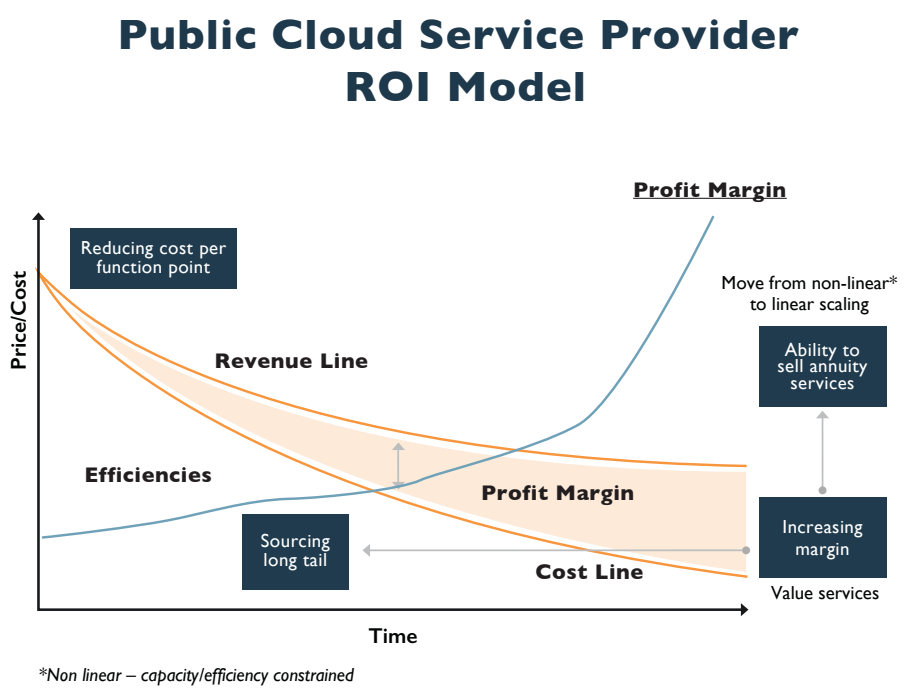



*Figure 1.10: Public Cloud Service Provider ROI Model*

# Cloud Computing Return on Investment

Although business alignment is paramount, cloud computing return on investment (ROI) must also be addressed. This metric should be addressed from multiple vantage points.

Cloud economic savings can be measured through the following key performance indicators (KPIs):

- Workload versus utilization
- Workload type allocations
- Instance to asset ratio
- Ecosystem optionality

The ROI model can also include operational metrics, such as:

- Speed of cost reduction
- Optimizing cost of capacity
- Optimizing ownership use

Business value can also be gleaned from process time reductions, product quality improvements, and customer experience enhancements. An ROI model example is shown in Figure 1.11.

## ROI Model Example

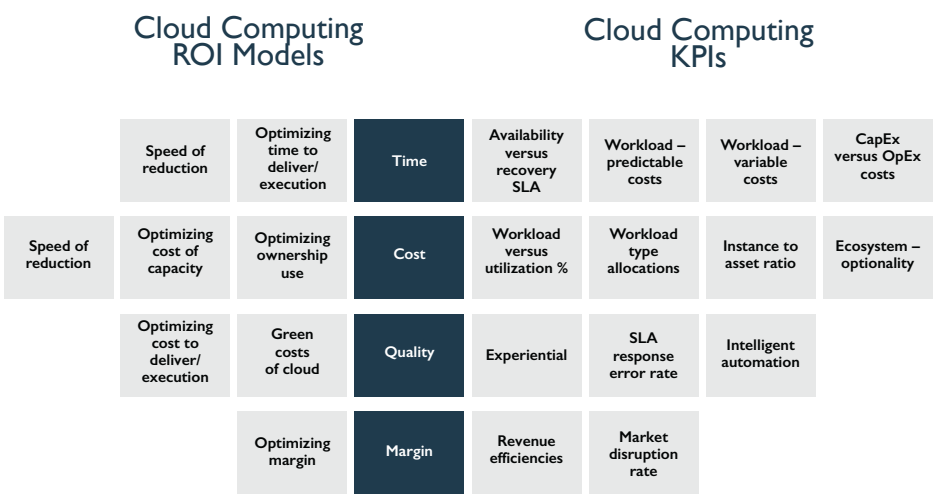



*Figure 1.11: ROI Model Example*

## Notes

Cloud Economic Model

**PPT**

**Cloud Computing Return on Investment (two slides)**

**PPT**

**ROI Model Example**

Notes

Cloud Economic Model

PPT

**Acquisition and Governance Changes**

# Acquisition and Governance Changes

A decision to adopt cloud computing will generally initiate far-reaching discussions about capital investment, IT budget allocations, IT acquisition, and enterprise governance. Cultural changes are also almost inevitable because these transitions normally result in some unique mixture of traditional enterprise IT, services from a Managed Service Provider, and cloud service consumption. When updating enterprise IT governance, corporate executives will have the task of codifying a proper middle ground among these very different operating models.

## Enterprise Cloud Transition Acquisition and Governance Changes

| Implementation Options | Capital Investment | Profit Model | Acquisition Model | Operational Governance |
|---|---|---|---|---|
| Enterprise IT | By Enterprise | N/A - Cost Center | RFP with Enterprise Selection of Best Vendor | Enterprise |
| Managed Service Provider | By MSP | Term Payments By Enterprise | RFP with Enterprise Selection of Best Vendor | Enterprise Enforced via Contract |
| Cloud Service Provider | By CSP | Marketplace Margin Leveraging Economies of Scale and Market Penetration | Enterprise Selection of Standing Service Options | CSP Offered SLA as Modified by Enterprise Negotiation |

*Table 1.2: Enterprise Cloud Transition Acquisition and Governance Changes*