



# **BACHELOR OF COMPUTER APPLICATIONS SEMESTER 6**

## **DCA3243 CLOUD COMPUTING**

# Unit 3

## Inside Cloud Computing

### Table of Contents

SL No	Topic	Fig No / Table / Graph	SAQ / Activity	Page No
1	<a href="#">Introduction</a>	-	-	3
	1.1 <a href="#">Objectives</a>	-	-	
2	<a href="#">Cloud Strategic Decisions</a>	<a href="#">1</a>	<a href="#">1</a>	4-8
3	<a href="#">Governance Issues</a>	<a href="#">2</a>	<a href="#">2</a>	9-16
4	<a href="#">Monitor and Management of the IT cost Effectively</a>	-	<a href="#">3</a>	17-21
5	<a href="#">Summary</a>	-	-	21
6	<a href="#">Terminal Questions</a>	-	-	22
7	<a href="#">Answers</a>	-	-	22-23

## 1. INTRODUCTION

With the help of new consumption and delivery models, cloud computing supports organisations to reduce costs and increase service levels. Like any other with a new evolution, cloud computing also comes with both challenges and opportunities. Understanding these issues is critical to achieving the expected benefits and walking further. Developing a business case is essential to support executive decision-making on whether and how to adopt a cloud solution. In this unit, we are going to discuss the sensational feelings of an organisation. Also, we had a discussion on strategic decisions in cloud computing. This unit also discusses cloud governance, the various governance issues, and how to overcome them. We are discussing how the monitoring of business processes helps to keep you on track to achieve your objectives. We are concluding this unit with a discussion on how to control and manage cloud IT costs effectively and efficiently.

### 1.1 Objectives

After studying this unit, you should be able to:

- ❖ *Identify the need for a cloud strategy.*
- ❖ *Demonstrate the cloud spectrum.*
- ❖ *Elucidate monitoring of business processes.*
- ❖ *Brief about the cloud IT cost management*

## 2. CLOUD STRATEGIC DECISIONS

### Why is Cloud strategy necessary?

The widespread adoption of cloud computing in the IT industry has significantly affected practically all types of enterprises.

IT executives and business leaders must develop a comprehensive cloud strategy for their companies. Making the Most of the Cloud Developing a business-driven decision framework and best practice IT operational models requires coordination across several areas.

This aids in standardising a company's cloud strategy while providing a method that will cater to the requirements of various use cases and business divisions.

The cloud strategy helps the business through the different phases of using or transitioning to cloud services while balancing the firm's benefits and carrying out effective risk management.

Using cloud services it offers to a broader range of customers through a self-service interface; cloud computing enables the speed and agility that digital enterprises today require. These cloud services encourage innovation and creativity among users.

The cloud strategy must also include the organisation's ultimate objectives and what is appropriate for the business's mission.

The idea is to adopt a cloud service from an outcomes viewpoint rather than seeing it as installing a set of technology.

A cloud strategy outlines a company's goals for its business and how it plans to achieve those goals.

"Having a cloud strategy will help you to apply its tenets fast with fewer delays, therefore quickening the arrival of your final business goals," claims Donna Scott, research vice president and distinguished analyst. It entails handling, organising, and processing numerous types of information.

A cloud strategy outlines the necessary business outcomes for the cloud and includes a plan for their realisation.

### How Organization will Consume Cloud Computing Services?

- Collaboration is made simple via cloud computing. In a cloud-based platform, team members may see and exchange information quickly and securely.
- Some cloud-based platforms even give employees across your organisation access to collaborative social areas, which boosts interest and engagement.
- The decision framework needs to be started with an awareness of the type of application and its technical aspects.
- Any effective cloud strategy will be built on this basis. The integration of the application and data with other systems, as well as the requirements and limitations of the linked data.

### The Hybrid Environments - Access, Secure, Manage, Integrate, Govern:

In a hybrid cloud, applications are executed in a mixed computing environment that combines computing, storage, and services from private and public clouds, as well as on-premises data centres and "edge" locations.

Organisations typically use various public cloud services, along with conventional applications, infrastructure, and possibly private cloud services.

As a result, a hybrid environment is created, which presents exceptional security, management, and governance problems.

The company's developers must create best practices and put tools into place to handle this type of hybrid environment. The distinct difficulties found while assessing particular use cases may also serve as a guide for further improvement and expansion of operational best practices.

### **The Impact on Existing Data Center and Infrastructure Approaches of the Organization:**

Taking care of data centre infrastructure can be a 24-hour task. Whether they are realistic expectations or not, your stakeholders are counting on 100% uptime. You feel more like a firefighter than a system administrator because of backups, security, resource use, and replacements. Planning can help relieve some of the pressure from your obligations.



Yet many firms will continue to value traditional data centres and infrastructure strategies. While utilising cloud computing, a deliberate move to infrastructure brokering is required.

Your data center's potential for growth may be constrained by a subpar architecture. Unexpected expansion that necessitates a data centre move can have a significant impact on costs and business continuity.

### **The cloud spectrum:**

Choosing the best cloud option for each organisation can be challenging because there are so many options available (including those that just offer partial cloud features).

Technology strategic planners must decide which choice best fits their stated demands and goals. Depending on the organisation and end goals, all cloud computing methods offer benefits, whether the strategy is 100% cloud-based or not.

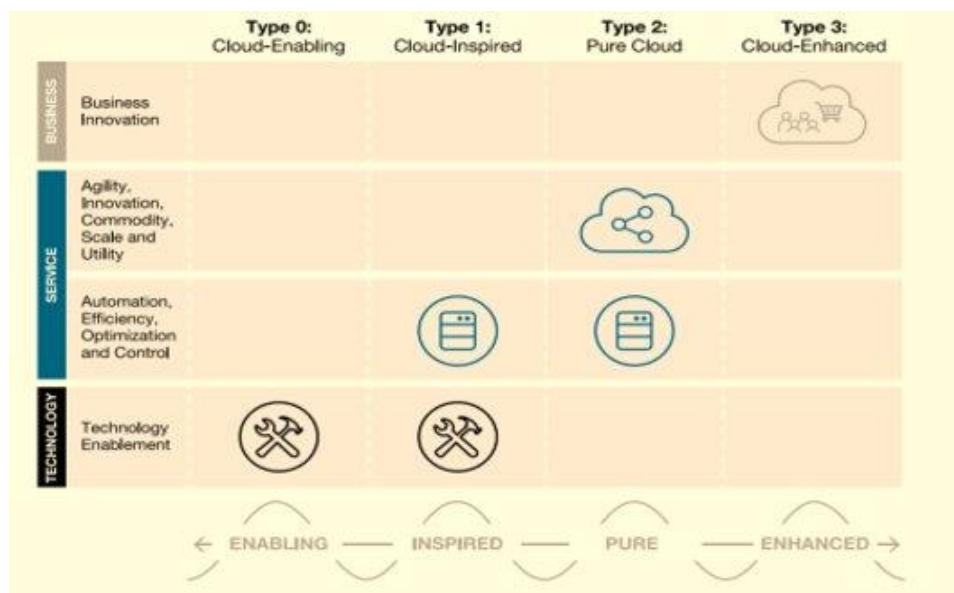
One must consider the capabilities created by the cloud spectrum. Broadly, the spectrum is classified into:

- Type 0
- Type 1
- Type 2
- Type 3

Depending on the business requirements, a particular type of cloud offering can be chosen. The details of each of these types will be covered in coming-up slides.

Cloud offerings have different types, as we already saw, each type represents a responsibility as seen below:

- Type 0 is cloud-enabling.
- Type 1, which is Cloud inspired.
- Type 2, which is Pure Cloud.
- Type 3, which is Cloud enhanced.



**Fig 1: Types of Cloud Offerings**

### The Guiding Principles for Cloud Adoption:

Organisations use cloud adoption as a strategic move to cut costs, reduce risk, and achieve scalability of database capabilities. Depending on the level of adoption, a company may have one or more levels of cloud adoption.

The company's IT management must establish a set of high-level guiding principles for the optimal process for cloud adoption and guidelines for what is expected of employees when they consider, implement, and use cloud services.

There are general ideas that can serve as a guide; however, these will be particular to each organisation.

Mainly, businesses had to think about how various adoption situations might appear.

### Migrating to the Cloud:

The process of partially or wholly transferring a company's digital assets, services, databases, IT resources, and applications to the cloud is known as cloud migration. Moving from one cloud to another is another aspect of cloud migration.

In contrast to other types of cloud migration (such as refactoring and rewriting, for instance), which typically offer more of these characteristics, it has been observed that many migrations to the cloud are "lift and shift" rehosting or other movements that do not exhibit

cloud characteristics at higher levels. New applications are the cloud's most frequent use case.

Separate cloud services from apps that are hosted in the cloud. There are "half steps" to the cloud that can be advantageous (there is no need to purchase hardware, for example). They need to provide the same results.

### **Is a Cloud Less Secure Than On-Premises Capabilities?**

Segmentation from user workstations is a significant security advantage the cloud provides over on-premises servers and infrastructure. Attackers most frequently enter networks using phishing and email-borne attacks. User workstations are almost always the entry point for the attacks.

It is thought that cloud computing could be more secure.

Nonetheless, there have only been a small number of security incidents in the public cloud so far; most incidents still involve on-premises data centre settings.

After cloud service providers have proven their capabilities, there is no reason to think their products won't be secure.

#### **SELF-ASSESSMENT QUESTIONS – 1**

1. The services which are provided by the cloud will influence your organisation either or\_\_\_\_\_.
2. Cloud computing enables organisations to reduce costs and improve service levels state [True/False].



### 3. GOVERNANCE ISSUES

Governance becomes more critical than ever for organisations utilising cloud services, according to the guide from ISACA, a non-profit global organisation focused on information systems assurance and security and enterprise governance. “Companies need to implement a cloud computing governance program to effectively manage increasing risk and multiple regulations and ensure continuity of critical business processes in the cloud”, according to ISACA.

In these economic times, executive management is excited about the potential for the cloud to reduce costs and increase the value of IT, but “getting that value is part of a good governance program,” said Jeff Spivey, international vice president of ISACA, and president of Security Risk Management Inc., a consulting firm based in Charlotte, N.C. “And making sure when you are getting the value, you manage the risk instead of jumping blindly off the cliff and hoping.”

An effective and efficient governance system is defined as a “system that facilitates the creation of an acceptable value to the various stakeholders using limited resources in a responsible way and at an optimal, or acceptable, level of risk to the various stakeholders”.

Governance objectives are defined as managing risks, value creation, and resource optimisation to achieve the enterprise goals.

#### ***Cloud Governance Consideration***

The first question that arose here is who should be responsible for assuring Cloud Security. If not already part of the business governance or system development life cycle process, the move to cloud computing essentially dictates that a company information security officer or director be included in all further governance and system development life cycle processes.

Will the adoption of cloud computing by organisations positively or negatively impact the ability of organisations to achieve their strategy? Will it impact the relationship between the organisation's business units, IT, and governance professions in aligning IT, risk management, and compliance with the organisation's strategy? One will need a more refined look at governance and cloud computing by examining organisation strategy and strategy alignment.

Will adopting cloud computing positively or negatively impact the ability of organisations to manage operational and technical risk? Will it motivate quicker deployment and reduce costs, impacting the ability of security and audit professionals to protect organisations? Will the reliance on service providers provide a better or reduced understanding of business risks?

Whether the adoption of cloud computing by organisations positively or negatively impacts the ability of organisations to create value by using their resources (technology, infrastructure, and people) in an optimal manner. Will it motivate for quicker deployment, and reduced costs impact resource value?

What questions should board members and executives consider when they are beginning to anticipate a movement to the cloud or planning to utilise cloud infrastructures, platforms, or services to support the organisation?

Our questions should encompass governance in terms of strategy, risk, and resource. We need to make sure that we address proper governance considerations. There are many challenges for assurance providers.

What can be done to improve the assurance professionals' ability to provide direct and indirect cloud computing users with trust in the software services and infrastructure that make up the cloud?

Some of the key assurance issues that need to be addressed are:

**Transparency:** Providers must demonstrate the existence of robust and effective security controls, assuring customers their information is properly secured against unauthorised access, change & destruction. How much transparency is enough and needs to be transparent?

**Compliance:** Concerns regarding data in cloud computing may not be stored in one place and may not be easily retrievable. Ensure that the data can be provided without compromising other information when it is demanded by the authorities.

**Trans-border information flow:** When information can be stored anywhere in the cloud, the physical location of the information can become an issue. Physical location dictates jurisdiction and legal obligation.

**Privacy:** It is imperative for providers to prove to customers that privacy controls are in place & demonstrate the ability to prevent, detect and react to security breaches in a timely manner.

**Certification:** Providers will need to provide assurance to their customers that they are doing the “right” things. Independent assurance from third-party audits and/or service auditor reports should be a vital part of any cloud computing program.

### ***Coping with governing issues***

Four distinct cloud categories exist, and each approach presents different governance challenges:

- Infrastructure as a Service
- Platform as a Service
- Software as a Service
- Business Process as a Service

To make it more complicated, these approaches have no clear dividing line. Emerging vendors often combine approaches into their contributions. In addition, in most instances, a hybrid situation develops where on-premises applications are used in collaboration with traditionally hosted services and cloud services. Governing internally provided services and externally provided cloud-based services introduces new challenges for a company's strategy:

How do you manage the overall lifecycle of your IT resources, including software licensing, cost allocation, and chargebacks? Protecting the integrity of your information resources and ensuring that you comply with data privacy rules and regulations. Make sure that all your service providers can prove and document that they are meeting governmental and corporate requirements.



**Fig 2: SPOT Framework**

There are four dimensions of cloud governance:

1. **Scope and Stakeholders:** Cloud providers, customers, enablers, resellers, and third-party providers are examples of operational stakeholders. Regulators, lawmakers, judges, non-governmental organisations, law enforcement, industry-standard bodies, and end users are examples of non-operational stakeholders.
2. **Policies and Process:** The rules by which businesses use the cloud and when computations and computer procedures are performed remotely.
3. **Organizations** means that businesses can innovate more quickly, drive business agility, streamline operations, and cut costs. It also means that businesses can scale and react quickly.
4. **Tools and Enabling Technologies:** Organizations are given the ability to access IT resources on demand, via the Internet, and on a pay-per-use basis, thanks to cloud computing. As a result, your business does not have to buy, set up, run, and upgrade hardware for physical data centres.
  - Companies that run services in the cloud implement a set of regulations and guidelines known as cloud governance. Enhancing data security, controlling risk, and facilitating the efficient functioning of cloud systems are the objectives of cloud governance.
  - Data security, system integration, asset deployment, and other facets of cloud computing are all properly planned for, considered, and managed thanks to cloud governance. Because cloud systems can be developed and managed by several



departments within a company, including outside vendors, and change frequently, they are very dynamic.

- Initiatives for cloud governance ensure this complex environment complies with regulatory requirements, business standards, and security best practices.

Cloud computing capacity, as well as its architecture, purchase, implementation, operation, and management. Best practices for Cloud Governance assist in maximising the organisations.

Effective governance is built on six governance principles for cloud-based applications. Every organisation has a different set of governance requirements. You should thus alter the policies stated below to suit your unique requirements.

- Financial management
- Cost optimisation
- Operational governance
- Performance management
- Asset and configuration management
- Security and Incident management

#### **The COBIT Model:**

- It stands for Control Objectives for Information and Related Technologies:
- The production of business value is addressed by IT governance (COBIT) through the optimisation of IT benefits, value delivery, risk, and resources. The Cloud Computing Governance Framework comprises elements of IT governance related to the value creation, advantages, risks, and resource optimisation of cloud computing.
- ISACA established a framework for IT management. IT (information technology) governance is the focus of the international professional organisation ISACA. Although ISACA currently just uses its acronym, it is still referred to in its IRS filings as the Information Systems Audit and Control Association.
- By implementing a single organization-wide governance, risk, and compliance (GRC) framework, COBIT 5 is a significant development in the governance of an organisation's IT. COBIT 5 will assist a new business by outlining a fast-track approach's road map.
- The following segments make up the three levels of the structure that COBIT creates:



- Business needs (information criteria), comprising attributes like reliability, compliance, confidentiality, and availability.
- Information technology (IT) resources, including infrastructure, applications, information, and people. IT processes, broken down into domains.

All sizes of organisations can benefit from using the COBIT framework:

- Enhance and uphold reliable data to aid in business decisions.
- Employ IT wisely to accomplish corporate objectives.
- Promote operational excellence by using technology.
- Make sure IT risk is effectively handled.
- Ensure that all laws, rules, and contractual obligations are followed.

SLA is an agreement between the cloud user and the cloud service provider.

Each cloud computing application must adhere to SLAs in the following three main technical areas:

Quality of Service (QoS) management, which is the issue of distributing resources to the mobile application to guarantee a high level of service towards performance and availability, is one of the difficulties brought on by cloud apps.

In Google Cloud, Application Integration is an Integration-Platform-as-a-Service (iPaaS) solution that provides a complete set of core integration capabilities to link and manage the plethora of apps and data needed to support diverse business activities.

A defined risk management approach is made possible by a combination of processes, people, and systems known as security governance. Insofar as it directly affects the security program, it consists of organisational structure, roles and duties, measurements, processes, and oversight.

A Cloud Computing governance platform encourages IT:

**To discover existing integration points:**

To give administrators a unified IT infrastructure for managing data and applications, cloud integration connects various cloud environments, systems, and applications. A hybrid

deployment strategy can be created by integrating public clouds with on-premises systems through cloud integration.

**To track integration dependencies:**

With the help of the intelligent component analysis platform Dependency-Track, businesses can pinpoint and lower risk in the software supply chain.

**An Azure example is** Open the web portal for the project where your team is defined. Choose Dependency Tracker from under the Boards group. To focus on your area of ownership, choose the area that corresponds to the team for which you want to view dependencies.

**To optimize less-than-ideal integrations:**

At its most basic level, cloud integration is the process of combining many cloud environments so that they may function as a single, integrated IT infrastructure for an organisation. This can be done through hybrid deployment or by using various public clouds.

The following are some of the issues that Cloud Governance features aid us in solving:

1. **Performance Management:** When a company uses cloud services, it is the service provider's duty to provide appropriate services and boost efficiency. The client's performance using the services will also suffer if the service provider falters. A proper governance cloud model, a set of regulations, and picking one of the top solutions can all help you avoid such situations.
2. **Governance/Control:** Your organisational strategies and business objectives can be supported by a sound set of policies and procedures. Both the business and the company's operating expenses will be improved.
3. **Security Issues:** One of the main issues is the security of the data. This is true because by following some tight guidelines, best practices, and regulations for cloud governance, security flaws can be prevented. To safeguard the information's privacy, availability, and integrity, a governance model should provide suitable authentication procedures. AWS and other cloud service providers are aware of a security flaw in the Kubernetes Kubectl tool that could allow a malicious container to overwrite or create files on a user's workstation due to the high number of security bug incidents in the cloud.

**Reasons for Cloud Governance:**

- Creates a cloud-based IT operating paradigm centred on the speed, agility, and cost of cloud computing, enabling cloud-speed business.
- Allows for friction-free, suitable cloud decision-making.
- Integrated with the enterprise IT governance procedures, rules, boards, and tools that are already in place.
- Achieving the benefits of clouds while providing fair and appropriate coverage of important decisions, investments, and risks.
- Proactive in identifying and stopping shadow clouds, as well as unapproved cloud activities that expose organisational hazards.

**SELF-ASSESSMENT QUESTIONS – 2**

3. Who can be included in the company's governance and system development life cycle process?
4. COBIT stands for \_\_\_\_\_.
5. \_\_\_\_\_ Will monitor operational security issues related to the cloud.

#### 4. MONITOR AND MANAGEMENT OF THE IT COST EFFECTIVELY

All IT departments monitor costs, but few monitor them in terms of asset performance, the requirement to optimise the return on investments for hardware and software. This is likely to change with the onset of cloud services. Unlike traditional licensing models, cloud propositions are based on rental arrangements.

Why is Cost Management required on the Cloud?

Today's cloud prices are hard to predict because decision-making in large enterprises is frequently de-centralized, and expenses are continually altering.

One of the main benefits of cloud computing is its capacity to scale quickly, but it also makes it simple for IT professionals to run applications without considering costs. Thus, implementing a cloud cost management strategy can aid a company in forecasting expenses and consumption.

Effective multi-cloud cost management that takes the expenses of various public cloud providers into account is crucial for enterprises that employ multi-cloud combinations.

A corporation may more successfully impose accountability throughout the organisation and enhance the functionality and effectiveness of its cloud technology by having a better awareness of expenses and usage.

You must compare two cost models:

- Operating expenses (paying per month, per user for each service)
- Capital investments (paying a purchase fee plus yearly maintenance for software that resides within your organisation)

Calculating the differences between the two cost models is a difficult process for most companies. In some situations, the new cost models shift some responsibility away from IT to the business unit. For example, in an organisation, when the email is managed in the cloud, if a company hires 20 new employees, the business unit needs to budget for 20 more users. Company IT need not ensure server capacity and IT staff are sufficient to support the additional users; here, this is the role of cloud providers. But IT belongs to a company that needs to monitor carefully whether the support of the cloud is effective.

Following are the steps followed to manage the cloud cost-effectively:

### **Step 1 – Gain visibility**

The management of cloud costs starts with the infrastructure specification. If you want to manage the cloud costs effectively, you need to be able to answer application-specific questions such as:

- What is the current configuration of nodes in a functional cluster?
- What is the cost of a functional cluster?

### **Step 2 – Define the blueprint.**

The next step is to standardise the infrastructure; most cloud applications are developed incrementally, resulting in non-standard configurations. This often happens because the lack of a consolidated view leads to variation in the process. For example, you may have started using a c1. Medium instance with 5GB EBS as a default node in your web server clusters but modified this configuration over time based on business needs.

To manage costs, you will need to formalise the blueprint, which reflects how you are going to deploy and configure your application on the cloud. Successful reference architecture should be accurate, covering the essentials of the infrastructure you will use, its costs, and projected capacity.

### **Step 3 – Manage capacity**

If the reference architecture provides the blueprint for your infrastructure, how are we going to measure the blueprint based on the business needs?

A successful capacity management policy should define the following:

- Configuration for each functional area of an architecture
- View on which functional area will be scaled.
- Scaling criteria for these dimensions (e.g., if disk usage exceeds 60%)
- The response to the criteria for scaling on each dimension (e.g., add additional node to cluster)

The key objective of a capacity management policy is to operate your infrastructure with a target level of efficiency. The closer you can manage to maximum utilisation of your cloud



resources without harming application availability, the more you get the best cost efficiencies.

#### **Step 4 – Rightsize**

With your reference architecture and capacity management policy defined, it is now time to choose the right size. Using your consolidated view, you can now identify the target infrastructure in one of these categories:

- Non-standard - infrastructure that deviates from the reference architecture
- Under-utilized - infrastructure that can be consolidated based on the capacity management policy
- Unused infrastructure - infrastructure that is used infrequently or not at all

#### **Step 5 – Optimize**

Your ability to optimise costs is limited to available options from your cloud provider. Amazon is the most mature in this area, providing two options:

1. Reserved instances - Reserved instances allow you to pay a reservation cost for your instances over a defined term (1 or 3 years) in exchange for guaranteed availability and a substantially reduced hourly cost. Reserved instances are useful for infrastructure expected to be always on based on the current and projected infrastructure needs of your application. Typical savings can be 40%+.

Spot instances - Spot instances allow you to purchase temporary instances from a marketplace, with the price determined by demand. Spot instances are useful for on-demand infrastructure, whose needs are short-term in nature and can be interrupted by unplanned termination (e.g., as the market price rises above your bid). The Cloud Cost Factors:

2. The price of your cloud migration is mostly determined by your current on-premises circumstances. These include your current infrastructure, workload integrations, cloud apps, the degree of function virtualisation, and the support you'll require during the transfer. For instance, if you employ an infrastructure with various customisations and a high reliance on your present infrastructure solution, shifting to the cloud infrastructure would take longer and demand more resources.
3. There are many factors, such as Virtual machine instances, memory, and storage, which affect the cloud, some of which IT teams initially overlook, which later increases the

public cloud bill. Fortunately, organisations can avoid any unwanted billing surprises with a smart cloud cost management strategy.

4. Costs increase as more people use the cloud. Some claim that cloud computing is more expensive than "the old way," yet this is really an apple to pears comparison. More flexibility, innovation, and cooperation are made possible by cloud computing.
5. We see it as an investment, and you can't afford to set it and forget it with investments.
6. Frequent reviews can minimise cloud expenses while gaining many advantages, particularly in the areas we listed below. All these elements must be taken into consideration by a solid cloud cost management approach.
7. Network traffic
8. Training and support
9. Web services and Software licenses

Cloud monitoring is a method of reviewing, observing, and managing the operational workflow in a cloud-based IT infrastructure.

The performance and availability of websites, servers, applications, and other cloud infrastructure are confirmed by manual or automated management procedures.

Prevent issues that can make it impossible for them to serve their customers.

Manual or automated IT monitoring and management techniques are performed to ensure that the cloud architecture or platform operates at peak performance.

You can use cloud monitoring to determine whether the performance of your cloud-hosted apps complies with their Service-Level Agreement (SLA), find out if there are any potential security risks, find out if there are any capacity issues, and evaluate expenses.

Prevent issues that could make it impossible for businesses to serve their clients.

Use manual or automatic IT monitoring and management techniques to make sure the cloud platform or structure is operating at its best.

**SELF-ASSESSMENT QUESTIONS – 3**

6. Linking internal and external processes together in a continuous way is the best way to ensure. Effective cloud-based \_\_\_\_\_ can capture performance issues before they happen. workload monitoring
7. Cloud licensing models are based on \_\_\_\_\_.

**5. SUMMARY**

Let us recap the content that we discussed in this unit so that for

- Influence of cloud service in your organisation, the status of various departments which get impacted by the cloud service.
- Strategic decisions on cloud computing help provide a decision framework that supports companies that are interested in migrating to cloud service.
- Governance becomes more critical than ever for organisations utilizing cloud services. In this unit, we are discussing various cloud governance issues.
- Various steps involved for effective cost management.

## 6. TERMINAL QUESTIONS

1. Discuss a few areas of an organisation that are affected by cloud computing.
2. Explain the concept involved in strategic decisions on cloud computing.
3. Discuss in detail the governance issues of cloud computing.
4. Brief the importance of monitoring business processes.
5. Discuss the steps involved in effective cost management.

## 7. ANSWERS

### Self-Assessment Questions

1. directly or indirectly.
2. True
3. security officer or director
4. 1) Segregation of Duties
5. Department of Homeland Security
6. customer satisfaction
7. rental arrangement.

### Terminal Questions

1. The services which are provided by the cloud will influence your organisation either directly or indirectly. And this impact is not only for the IT department. (For more details, refer to section 3.2)
2. The strategy is based on a principle and risk approach. It is both tactical and strategic. (For more details, refer to section 3.3)
3. Companies need to implement a cloud computing governance program to manage increasing risk and multiple regulations effectively. (For more details, refer to section 3.4)
4. It supports work assignment through skills-based routing; relevant content will be available for each and helps track pending work and monitor process performance and user productivity. (For more details, refer to section 3.5)
5. IT cost management helps the organisation to monitor in terms of asset performance and requirements to optimize the return on investments. (For more details, refer to section 3.6)

**E-References:**

- <http://www.pwc.com/us/en/issues/cloud-computing/functional- changes.HTML>
- <http://www.cloud.Business Impact of Cloud Computing – Accenture Outlook.htm>
- <http://www.isaca.org/Groups/Professional-English/information-securirty-management>
- [http://searchcloudsecurity.techtarget.com/news/2240038839/ISACA- releases-cloud-computing-governance-guide.](http://searchcloudsecurity.techtarget.com/news/2240038839/ISACA- releases-cloud-computing-governance-guide)
- <http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf>

