



BACHELOR OF COMPUTER APPLICATIONS

SEMESTER 6

DCA3243

CLOUD COMPUTING

Unit 4

Cloud Service Administration

Table of Contents

SL No	Topic	Fig No / Table / Graph	SAQ / Activity	Page No
1	<u>Introduction</u>	-	-	3
	1.1 <u>Objectives</u>	-	-	
2	<u>Service Level Agreements</u>	-	<u>1</u>	4-8
3	<u>Support Services</u>	-	<u>2</u>	9-10
4	<u>Accounting Services</u>	-	<u>3</u>	11-12
5	<u>Resource management</u>	<u>1</u>	<u>4</u>	13-21
	5.1 <u>IT security management</u>	-	-	
	5.2 <u>Performance management</u>	-	-	
	5.3 <u>Provisioning</u>	-	-	
	5.4 <u>Security</u>	-	-	
6	<u>Service Management</u>	-	-	22
7	<u>Summary</u>	-	-	23
8	<u>Terminal Questions</u>	-	-	24
9	<u>Answers</u>	-	-	24-25

1. INTRODUCTION

As per our previous unit's discussion, we can understand that cloud computing plays a vital role in the initiation of modernised Information technology by identifying enterprise-wide common services and solutions and, based on which it develops a new cloud computing business model. The main objective of this process is that these models should support reusability, and based on the situational demand, they should satisfy the needs. This initiative is service based; hence, the infrastructure, data, application and solutions can be shared across the organisation to achieve reusability. Since cloud computing offers reusability, it is able to provide the organisation with a cost-effective, service-oriented approach by sharing various computing resources. In this unit, we are discussing the service level agreement role and how effectively we can monitor. We also discussed the various cloud services like accounting services and support services and how to manage resources like IT, performance, and service. We are going to conclude this unit with a discussion of the scenario of software dependencies in the cloud.

1.1 Objectives

After studying this unit, you should be able to:

- ❖ Explain the service level agreement.
- ❖ Discuss various cloud support services.
- ❖ discuss cloud accounting services.
- ❖ Brief about cloud service management and software dependencies

2. SERVICE LEVEL AGREEMENTS AND MONITORING

A company needs to expect the unexpected. Generally, companies face new and unexpected challenges. We cannot avoid such a situation, but we can overcome it if we create a strong initial set of ground rules and plans for the exceptions. Challenges may reach you from different directions, such as networks, processing power, security challenges, availability of resources, and even legal issues. As cloud customers, we operate in environments that can span networks, geographies, and systems. It only makes sense to agree on the desired service level for your customers and measure the real results.

Companies that buy cloud services from service providers must accept the service level agreement. A service level agreement is a contract that specifies the type of service that you are going to avail from providers and what the penalties will be during an unexpected business interruption. Internet service providers will generally include service-level agreements within the terms of their contracts with customers to define the level(s) of service that was sold in general language terms. In this case, the SLA will typically have a technical definition in terms of mean time between failures (MTBF), mean time to repair or mean time to recovery (MTTR), various data rates, throughput, jitter, or similar measurable details.

Organisations should not commit mission-critical systems to the cloud without negotiating an SLA that includes significant penalties for not delivering the promised service level. Organisational management should understand what type of service will be suitable for changing business conditions. Here, the management can assume that the service will provide the service required by the organisation in the event it changes its business.

In some sense, the SLA sets expectations for both parties and acts as the roadmap for change in the cloud service, both expected changes and surprises. Just as any IT project, which would have a roadmap with clearly defined deliverables, an SLA is equally critical for working with cloud infrastructure. This situation forces us to discuss what should be in SLA.

To consistently develop an effective SLA, the following is the list of important criteria that need to be established.

- Availability (e.g., 99% during workdays, 98% for nights/weekends)

- Performance (e.g., maximum response times)
- Security/privacy of the data (e.g., encrypting all data which are transmitted and stored)
- Disaster Recovery expectations (e.g., recovery commitment for worst case)
- Location of the data (e.g., reliable according to local legislation)
- Access to the data (e.g., readable format retrieval from the provider)
- Portability of the data (e.g., Movement across different providers)
- Process to identify problems and resolution expectations (e.g., call centre)
- Change Management process (e.g., changes – new or updated services)
- Dispute mediation process (e.g., escalation process, consequences)
- Exit Strategy with expectations on the provider to ensure a smooth transition.

A contract with an IT vendor must include SLAs. An SLA compiles details about each contracted service and the expected reliability of those services into a single document.

The types of SLA:

There are two types of SLAs from the perspective of application hosting.

- **Infrastructure SLA:** The infrastructure manager oversees and provides assurances for the availability of the infrastructure, including server equipment, power, network connectivity, etc. Applications that are installed on these server machines are managed by the businesses themselves. Customers lease equipment, which is separated from equipment belonging to other clients.
- **Application SLA:** The Service Level Agreements application allows you to create and manage service level agreements. Service level agreements contain the terms of the agreements between clients and service providers. Services are tasks that service providers complete in order to satisfy customer needs. To sustain service level agreements, service providers must fulfil certain requirements. The server capacity is made accessible to the apps under the application co-location hosting model exclusively on the basis of their resource requirements. Because of this, the service providers can arbitrarily distribute and remove computing resources among the co-located apps. To ensure that their customers' application SLAs are met, service providers must also take responsibility for this.

The different levels of SLA:

1. Customer-based SLA: It is possible to address customer-specific problems. One or more organisational departments have greater security standards. For instance, due to its essential position and management of financial resources, the finance department requires additional top security measures.
2. Service-based SLA: Any concerns pertaining to a particular service (with respect to the client) can be addressed. This applies to all clients who contract the same service, such as when all clients of a specific IP telephony provider contract for IT support services.
3. Multilevel SLA: When a large firm has a multi-level structure, less work is duplicated while allowing for customer and service customisation.
4. Corporate-level SLA: The general difficulties affecting the organisation are all addressed, and they apply to the entire company. For instance, a security SLA at the organisational level might require each employee to set passwords of 8 characters and to change them every 30 days (about four and a half weeks), or it might require each employee to have an access card with a photo imprinted on it.

A typical SLA will contain the following components:

- Type of service to be provided.
- The service's desired performance level, especially its reliability and responsiveness. Monitoring process and service level reporting
- The steps for reporting issues with the service
- Response and issue resolution timeframe
- Repercussions for the service provider not meeting its commitment

Steps r Reporting Issues with the Service:

Under Reports > Email SLA Report or by choosing SLA from a device action menu, you can set up an SLA Report for a monitoring device. By adjusting the SLA report parameters from this screen, you can further alter the report's appearance.

- This service level reporting helps monitor SLA compliance of IT components and/or services, and this part of the SLA will specify the contact details to report the problem.
- Also, the order in which details about the issue must be reported and the contract will also include a time range in which the problem will be investigated and when the issue will be resolved.

SLAs can contain numerous service-performance metrics with corresponding service-level objectives (SLOs).

Commonly agreed metrics in these cases include:

- **Abandonment Rate:** Percentage of calls abandoned while waiting to be answered.
- **ASA (Average Speed to Answer):** Average time (seconds) it takes for a call to be answered by the service desk.
- **TSF (Time Service Factor):** Percentage of calls answered within a definite timeframe. e.g., 80% of calls answered in 20 seconds.
- **FCR (First-Call Resolution):** Percentage of incoming calls that can be resolved without the use of a callback or without having the caller call back the helpdesk to finish resolving the case.
- **TAT (Turn Around Time):** Time taken to complete a certain task.
- **TRT (Total Resolution Time):** Total time taken to complete a certain task.
- **MTTR (Mean Time to Recover):** Time taken to recover after an outage of service.

The SLA Life cycle:

- Each SLA goes through a sequence of steps starting from identification of terms and conditions, activation and monitoring of the stated terms and conditions, and eventual termination of the contract once the hosting relationship ceases to exist.
- The lifetime of a service level agreement (SLA) guides it from its identification at the initial level to its activation and, ultimately, when it is no longer necessary, and the lifecycle of a service level agreement can be followed via an SLA object.
- Such a sequence of steps is called the SLA life cycle and consists of the following five phases:
 1. Contract definition
 2. Publishing and discovery
 3. Negotiation
 4. Operationalization
 5. De-commissioning

The performance guarantee agreed upon by the client and cloud services provider is known as a Service Level Agreement (SLA). All Service Level Agreements in cloud computing were previously negotiated between a client and the service consumer.

SLA management of applications hosted on cloud platforms involves five phases:

1. Feasibility
2. On-boarding
3. Pre-production
4. Production
5. Termination

SELF-ASSESSMENT QUESTIONS – 1

1. SLA Stands for _____ .
2. _____ is the agreement with an individual customer group by covering all the services they utilise.
 - a. Customer-based
 - b. service-based
 - c. Level-based
 - d. customer level based.
3. An SLA is a contract that specifies only the type of service that you are going to avail from providers. State [True/False]

3. SUPPORT SERVICES

When the organisation moves towards the cloud for its applications or infrastructure, it doesn't mean that it doesn't require any service support. With the support of the latest technology, the needs of the users are also increasing. Customers are expecting more and better services from the service providers, which need to be delivered through possible channels. The organisation needs to make sure that support targets are agreed on in advance with a cloud services provider. Thus, your company must align its internal support team that deals with internal customers with the cloud provider.

Just consider the situation where some important application has a performance problem. Especially in a hybrid environment, it's not always easy to tell if a problem resides within the cloud or outside of it. Such situations need to be prevented or at least handled in a very efficient manner. This may be the reason more companies are using salesforce.com customer service, which provides software as a service solution for call centres for customer relation management and desk management. The main advantage of the method compared to traditional customer support is here.

The support is delivered by subscription over the web, whereas in the traditional method, it is based on premises. The process involved in hardware or software purchase, maintenance, deployment or your agents are not required.

For a better understanding of the cloud support service, we will discuss the support provided by one of the leading cloud computing providers, AWS (Amazon Web Services). Let us now discuss the premium support offered by AWS. Its scope is to explore the best practices that help integrate, deploy, and manage applications in the cloud. To troubleshoot the API issues, operational and systematic problems with various resources are provided, as well as best practice recommendations to improve efficiency and performance.

Client-side diagnostic tools: In case of apparent networking or performance issues, you can accelerate the troubleshooting process by running these diagnostics and output files can be shared with them.

Technical Account Manager (TAM): This provides technical expertise for the complete range of AWS services and obtains a detailed understanding of your use case and technology

architecture. It works with AWS Solution Architects in launching new projects and recommends best practices throughout the implementation life cycle. Your TAM will act as the primary point of contact for ongoing support needs, and you will have a direct telephone line to your TAM.

TAM management business review: responsible for helping you in planning, executing, and evaluating your infrastructure performance. Conducts regular performance assessments, participates in requested meetings, and collaborates on new launches to ensure readiness.

Apart from the above, general cloud support is needed for the following activities: system operation services, CRM, ERP, workflow development and management software, data centres, cloud platforms, cloud clients, and database linking tools.

SELF-ASSESSMENT QUESTIONS – 2

4. _____ customer service, which provides software as a service solution for most of the companies.
5. _____ provides technical expertise for the complete range of AWS services.
6. TAM management business review responsible for helping you in _____.
 - a. Planning
 - b. executing
 - c. Evaluating
 - d. All the above

4. ACCOUNTING SERVICES

Catching Clouds bundles and integrates a range of cloud accounting services to provide solutions that can be adapted to your business. These services enable you, your team, and Catching Clouds' virtual controllers and bookkeepers access to your accounting data.

Core cloud accounting services: These cloud accounting services comprise the core services that are included in every solution by the catching cloud providers

Hosted accounting software: It takes care of all the hosting accounting services in the cloud; a secure data centre permits your business to access the data from anywhere and anytime.

Secure online portal and document management system: It plays a major role in optimising your business towards being paperless and shifting your accounting documents to the cloud. It also supports migrating your current data. All accounting support documents can be linked to your QuickBooks file and will be stored safely in the cloud.

Online accounts receivable/payable Online accounts receivable and payable cloud service simplifies and automates vendor bill payment and customer invoicing. This service is also supported to reduce the time involved in paper processes and integrates with the hosted accounting solution.

Additional cloud services

These additional services may or may not be applicable to your organisation, but these are available to support your business. These additional cloud services can be included in your business at any point in time when you require them.

Cloud document management: Most businesses today are interested in becoming "paperless" to improve efficiency and reduce costs. Cloud computing service helps to move all of your business data to the cloud and install and set up the processes to improve your efficiency by managing your workflow. This will provide backups of all your data and the ability to work remotely for you and your employees, as well as an easy way to share data with your customers and vendors.

Time & Expense: This service speeds up and simplifies how you track time, manage project accounting, invoice clients and create expense reports. The intuitive online platform helps to avoid manual entry and paperwork by seamlessly integrating with your back-office systems for accounting, document management, bill payments, and payroll. This service may also integrate with the hosted accounting solution.

Supported Services

The following services are critical to most businesses.

Payroll: Catching Clouds understands that payroll is a key component of every business, works closely with the major payroll and PEO providers, and integrates where possible.

Sales Tax: Sales Tax is a service that applies to most businesses. The online tools will reduce time and ensure compliance where you need to manage sales tax in more than one jurisdiction. This service reduces audit risk with cloud-based sales tax services that make it easy to manage exemption certificates, calculate rates, file forms, and remit payments. This service saves time and cost by addressing the time-consuming process of identifying the sales tax requirements across the country.

SELF-ASSESSMENT QUESTIONS – 3

7. Online accounts receivable and payable cloud service simplifies and automates vendor _____ and.
8. _____ service speeds up the process and simplifies your tracking time.

5. RESOURCE MANAGEMENT

There is not much difference between the cloud-services-based resources and the resources from your own environment, except that they stay remote. Preferably, you have a complete view of the resources you use today or may want to use in the future, but this is not easy to achieve practically.

In most cloud service environments, the customer is able to access only the services they're permitted to use. Entire applications may be used on a cloud services basis, whereas development tools are sometimes cloud-based. In fact, testing and monitoring environments can be based on the

cloud. In this situation, how are cloud users or customers going to manage their cloud resources? Now we are going to discuss the three aspects of cloud resource management where it applies:

- IT security
- Performance management
- Provisioning

5.1 IT Security Management

Since cloud computing represents a new computing model, there is a great challenge of uncertainty about how security at all levels, like application, network, host, and data level, can be achieved. This uncertainty leads the information executives to state that security is their number one concern with cloud computing. However, the cloud service provider implements its own IT security procedure by protecting customers from external threats and safeguarding the individual customer environments isolated from one another.

When looking at the network level of infrastructure security, it is important to distinguish between public clouds and private clouds. In the case of private clouds, there are no new attacks, vulnerabilities, or changes in risk specific to this topology that information security employees need to consider.

Your organisation's IT architecture may change with the implementation of a private cloud, but it is not necessary that the current network topology change accordingly. If you have a

private extranet in place, for practical purposes, you probably have the network topology for a private cloud in place already. The current security considerations will also be applied to private cloud infrastructure. And the security tools you have in place are also necessary for a private cloud and operate in the same way.

For every type of cloud service, the provider delivers a good deal of IT security. You may need to understand how the cloud provider handles issues such as patch management and configuration management as the provider upgrades to new tools and operating systems. Customers need to understand that the hardware and software are properly provided by the cloud providers in terms of firewalls, intrusion detection systems, VPNs, and secure connections. Need to know how the providers are protecting the overall environment. In the case of Infrastructure as a Service and Platform as a Service, cloud providers need to clarify the kind of IT security they expect the customer to put in place on their own behalf. With Software as a Service, the provider is responsible for all security except for access security, either an identity management system or at least a local access control application through the customer's own systems.

IT service management (ITSM) is a set of policies and practices for implementing, delivering, and managing IT services for end users in a way that meets the stated needs of end users and the stated goals of the business.

Planning ease is one of the simplification requirements. You can simply oversee and manage your monthly IT expenses with cloud-based ITSM. It makes it simpler to implement IT services in your company and to construct systems.

The organised integration of security within an organisation is referred to as ITIL security management.

Information security management is the process that "aims to secure the confidentiality, integrity, and availability of an organisation's information, data, and IT services," according to the Information Technology Infrastructure Library (ITIL). A more comprehensive aspect of corporate security management strategy than that of an IT service provider.

Benefits of IT security:

- IT security prevents malicious threats and potential security breaches that can have a huge impact on the organisation.
- When you enter your internal company network, IT security helps ensure only authorised users can access and make changes to sensitive information that resides there.
- IT security works to ensure the confidentiality and integrity of your organisation's data.
- Cloud security is a set of control-based safeguards and technology protection designed to protect resources stored online from leakage, theft, or data loss.

Information technology security is information security used in computer systems and technology. It emphasises guarding against unauthorised access to or destruction of computers, networks, programs, and data. Cybersecurity is another name for IT security.

- Network security: Network security is about getting your network secure from unauthorised or malicious users. This will ensure that usability, reliability, and integrity are uncompromised.
- Internet security: Internet security refers to the protection of information that is sent and received in browsers, as well as network security involving web-based applications. These protections are designed to monitor incoming internet traffic for malware as well as unwanted traffic.
- Endpoint security: Endpoint security is a type of security that provides protection at the device level. Devices that may be secured by endpoint security include cell phones, tablets, laptops, and desktop computers.
- Cloud security: Cloud providers can attempt to avoid cloud security issues with the service they provide but can't control how customers use the service, what data they add to it, and who has access.
- Application security: Cloud application security is a series of defined policies, processes, controls, and technology governing all information exchanges that happen in collaborative cloud environments like Microsoft Office 365, Google G Suite, Slack, and Box.

The CIA Triad is actually a security model that has been developed to help people think about various parts of IT security.

- Confidentiality refers to preventing the disclosure of information to unauthorised individuals or systems, enforced usually by encryption and by restricting access to the places where it is stored.
- Integrity in information security means maintaining and assuring the accuracy and consistency of data over its entire life cycle, implying that data cannot be modified in an unauthorised or undetected manner.
- Availability means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly and always available, preventing service disruptions due to power outages, hardware failures, and system upgrades.

Components of Developing a Strong Information Security Program:

- Apply defence measures: Assess the security controls to identify and manage risk.
- Establish a culture of security: Develop a sound Security Awareness program.
- Measure your Information Security Program by developing meaningful metrics.
- Develop and implement an Incident Response Plan.

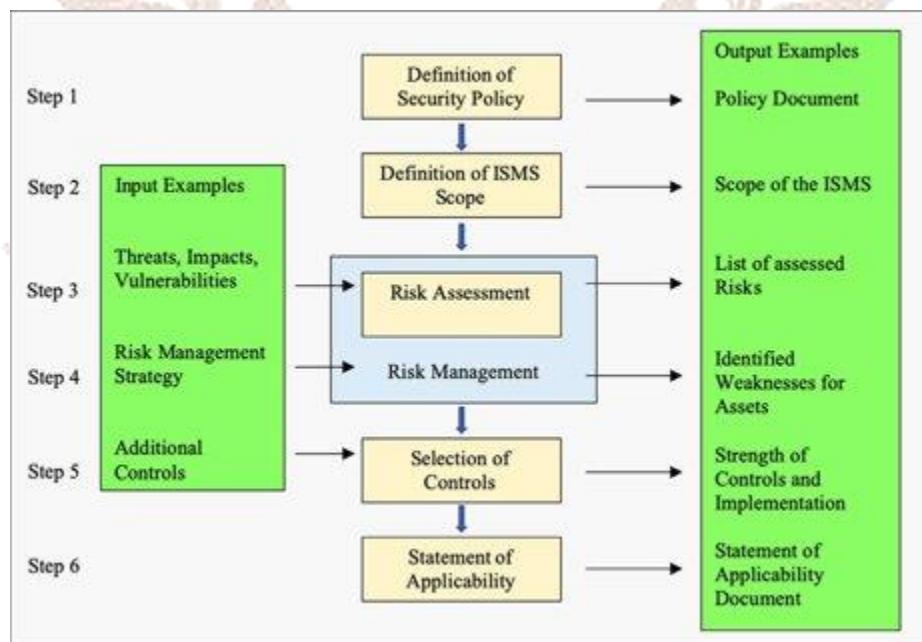


Fig 1: ISMS Framework

The creation of an ISMS framework requires the following six processes, as depicted in the above figure:

- Definition of Security Policy,
- Definition of ISMS Scope,
- Risk Assessment (as part of Risk Management),
- Risk Management,
- Selection of Appropriate Controls and
- Statement of Applicability

The key components of the ISMS are steps 3 and 4, which deal with risk assessment and management. These steps "transform" security policy targets into specific plans for the implementation of controls and mechanisms that are designed to reduce threats and vulnerabilities while also dealing with the rules and guidelines that govern security policy.

Information hazards are unrelated to the procedures and tasks associated with stages 5 and 6. They are more closely tied to the operational procedures necessary for the technological deployment, upkeep, and management of security measures.

Finally, it should be noted that while the ISMS is a repeatable process overall, steps 1 and 2 typically have longer recurrence cycles than steps 3, 4, and 6 in the majority of the above-mentioned organisation types. The fundamental reason for this is that, while the Risk Management process is ultimately a "daily" operational matter, the formation of a security policy and the specification of the ISMS scope are more frequently management and, to a certain extent, strategic issues.

5.2 Performance management

Performance management is all about how your software services run effectively inside your own environment through the cloud. If you start to connect software that runs in your own data centre directly to software that runs in the cloud, it creates a potential bottleneck at the point of connection.

You may change the basic data centre network topology and some application configurations when you move applications or services into the cloud. It reflects that the performance needs to be considered and designed in the beginning for every type of cloud service like

Infrastructure Service, Platform Service, and Software Service. Otherwise, services connected between the cloud and your computing environment will have an impact on performance. Similar conditions are applicable where there are data translations or specific protocols to adhere to at the cloud gateway. As a customer, your ability to control the resources directly will be much lower in the cloud. Therefore,

- The connection points between various services must be monitored in real-time. Through this, you can avoid the breakdown of the business process.
- The connection points are expected to have expanded bandwidth

From the performance perspective, the situation is likely to be much less delicate if systems don't connect the data centre and the cloud. Many companies combine services in the cloud and services within their own data centre. Thus, monitoring across these environments prevents many problems.

According to Jay Prassl, VP of Marketing at SolidFire, Performance management in the cloud is defined as "We focus on solving a very specific problem in the cloud, which is the ability to guarantee performance to the high-performance applications in a really large environment. The concert of performance management, inline efficiencies, and system automation - when you combine these three things together, you get a powerful play in the cloud provider space".

5.3 Provisioning

With Software as a Service, a customer expects the provisioning of extra services to be immediate, automatic, and effortless. However, the cloud service provider is accountable for keeping an agreed-on level of service and provisions of resources.

The situation is similar to Platform as a Service or Infrastructure as a Service, but you may need to directly request additional resources because, in both cases, customers are directly managing the cloud resources instead of having them managed on your behalf. Software workloads vary throughout the day, week, month, and year in the data centre in the normal situation. Unexpectedly high peaks can be managed with the supply of required capacity on time. Immediate attractions on infrastructure as a service are the data centres that can pay for additional or extra resources on demand and move their volatile workloads into the

cloud. In other words, the hardware used in the data centre is much more efficient and capable.

The resource provisioning within Cloud data centres influenced market-oriented principles. Very efficient resource allocation mainly depends on user QoS (Quality of Service) targets and workload demand patterns. There are many critical QoS parameters that need to be considered in a service request, like reliability and trust/security. QoS requirements need to be dynamically updated over time and cannot be static due to continuous changes in business operations and environments. Customers need to be considered more since they are paying to access services in data centres. The approach to realisation vision consists of the following:

- Support for customer-driven service management based on customer profiles and QoS requirements.
- “Definition of computational risk management tactics to identify, assess, and manage risks involved in the execution of applications with regards to customer needs and service requirements.
- Strategies need to be designed, considering both customer-driven service management and computational risk management to withstand SLA-oriented resource allocation.
- incorporation of autonomic resource management models should effectively self-manage changes in service requirements to satisfy both new service demands and existing service obligations.
- Virtual Machine (VM) technology is to dynamically assign resource shares according to service requirements.
- Developed resource management strategies and models needs to be implemented to real computing server in an operational data centre”.

The process of cloud provisioning can be conducted using one of three delivery models.

- Each delivery model differs depending on the kinds of resources or services an organisation purchases, how and when the cloud provider delivers those resources or services, and how the customer pays for them.

These three provisioning models are the following:

1. Advanced provisioning
2. Dynamic provisioning
3. User self-provisioning

Now the question arises: Why does Cloud Provisioning Matter?

While traditional on-premises technology can exact large upfront investments from an organisation, many cloud providers allow customers to pay for only what they consume.

Cloud provisioning offers numerous benefits to organisations that aren't available with traditional provisioning approaches.

A commonly referred benefit is scalability. In the cloud provisioning model, however, organisations can simply scale up and scale down their cloud resources based on short-term usage requirements. Organisations can also benefit from the speed of cloud provisioning.

For example, an organisation's developers can quickly spin up an array of workloads on demand, removing the need for an IT administrator who provisions and manages computer resources.

Potential cost savings are another benefit of cloud provisioning.

5.4 Security

Security in cloud service administration is crucial due to the sensitive nature of the data and systems involved. Here are some key aspects to consider:

Data Encryption: Ensure data encryption both in transit and at rest. Use strong encryption algorithms to protect sensitive information from unauthorised access.

- **Access Control:** Implement strict access controls and identity management. Use multi-factor authentication role-based access control (RBAC) and regularly review and update access permissions.
- **Regular Audits and Monitoring:** Continuously monitor the cloud environment for anomalies or suspicious activities. Conduct regular security audits and assessments to identify and address vulnerabilities.

- Compliance and Regulations: Understand and comply with industry-specific regulations and standards (such as GDPR, HIPAA, etc.) to ensure that your cloud service meets the necessary requirements.
- Secure Configuration: Follow best practices for configuring cloud services securely. This includes using strong passwords, limiting unnecessary access, and regularly updating software and systems.
- Backup and Recovery: Have a robust backup and disaster recovery plan in place. Regularly back up data and test the recovery process to ensure business continuity in case of a security breach or data loss.
- Patch Management: Keep all software and systems updated with the latest security patches to protect against known vulnerabilities.
- Incident Response: Develop and document a clear incident response plan to effectively respond to security incidents. This should include procedures for containing the incident, investigating, and mitigating its impact.
- Vendor Security: If using third-party services or vendors, ensure they adhere to strong security practices. Vet their security measures and protocols before integrating their services into your cloud infrastructure.
- Employee Training: Educate employees about security best practices, including phishing awareness, data handling, and the proper use of cloud services.

Remember, security in cloud service administration is an ongoing process that requires constant attention and adaptation to evolving threats and technologies.

SELF-ASSESSMENT QUESTIONS – 4

9. The basic data centre network can be changed when you move applications or services into the cloud. State [True/False]
10. Customers' expectation for provisioning extra service to be
 - a. immediate
 - b. automatic
 - c. effortless
 - d. All the above
11. _____ Technology is used to dynamically assign resource shares according to service requirements.

6. SERVICE MANAGEMENT

When you look at the cloud in common understanding, it is a combination of private, public and hybrid clouds in IT environments, which leads to IT services. These services are available at different layers, like common segmentation into SaaS, PaaS, and IaaS, which is about the production of standardised reusable services. Cloud Computing is all about using these services. It is about procurement, management, orchestration, accounting, and so on. In a perfect world, all services of all products (internal and external) would be managed consistently. However, the service management aspect of Cloud Computing appears not to be at the centre of most discussions around Cloud Computing. Many discussions are just about tactical comparisons and views of parts of Cloud Computing. Many discussions are around security. In this context, service management covers all the operations of data centres. This considers necessary tools and techniques for managing services by the cloud providers as well as organisation internal members across IT, Physical and virtual areas. Service management widely covers many disciplines like configuration management, capacity planning, network management, asset management, service desk workload management, root cause analysis and patch & update management.

The reality is that the cloud itself is a service management platform. Therefore, well-designed cloud service portfolios include a tight integration of the core service management capabilities and well-defined interfaces.

7. SUMMARY

Let us recap the content that we discussed in this unit:

- Service level agreement is a negotiated agreement between the service providers and the user. Here, there is an agreement between two parties called a contract. SLA consists of service definition, measurement of performance, problem management, customer duties, warranties, recovery from disaster, and agreement for termination.
- Cloud computing service supports their clients in utilising current technologies and helps to ensure business continuity within efficient cost limitations.
- Cloud accounting supports a no-manual accounts service; it provides best practices to manage financial transactions through security and access to internet software anywhere.
- Resource management helps to bring an optimal solution between energy saving and the delivered performance.
- IT provides solutions for virtualised network security platforms and supports applications and infrastructure to keep the data safe. Supports maintaining confidential matters from public access. Provides visibility to cloud providers
- Untangling software dependencies arise when your organisation plans to move fully or a part of a system towards the cloud.

8. TERMINAL QUESTIONS

1. What is SLM? Explain its role.
2. Discuss the cloud support services in detail.
3. Explain cloud accounting services.
4. Discuss cloud resource management.
5. Elucidate cloud service management.

9. ANSWERS

Self-Assessment Questions

1. Service level agreement.
2. a. Customer based.
3. False
4. salesforce.com
5. Technical Account Manager
6. All the above
7. Bill payment and customer invoicing.
8. Time & Expense
9. True
10. d. All the above
11. Virtual Machine
12. private, public and hybrid

Terminal Questions

1. A service level agreement is a contract that specifies the type of service that you are going to avail from providers during an unexpected business interruption. For details, refer to section 2.
2. Cloud is provided with various support services to handle the technical issues that may be faced by the organisation; for details, refer to section 3.
3. Catching Clouds bundles and integrates a range of cloud accounting services to provide solutions that can be adapted to your business. For details, refer to section 4.
4. Entire applications may be used on a cloud services basis, whereas development tools are sometimes cloud-based. For details, refer to section 5.

5. It is about the production of standardised reusable services. For details, refer to section 6.

E-References:

- http://knoesis.wright.edu/library/download/OOPSLA_cloud_wsla_v3.pdf
- <http://www.wired.com/cloudline/2011/12/service-level-agreement%E2%80%99s-in-the-cloud-who-cares>
- <http://blogs.kuppingercole.com/kuppinger/2010/10/28/cloud-computing-is-mainly-service-management/>
- <http://smart421.wordpress.com/2011/01/07/service-management-in-cloud-and-virtual-environments/>