



IBM Cloud Computing Professional Certification Program

Study Guide Series

Exam C2030-284 – Foundations of IBM Cloud
Computing Architecture V4

Purpose of Exam Objectives	3
High-level Exam Objectives	4
Detailed Exam Objectives	6
Section 1 - Cloud Computing Concepts and Benefits.....	6
Section 2 - Cloud Computing Design Principles	18
Section 3 - IBM Cloud Computing Architecture.....	28
Section 4 - IBM Cloud Computing Solutions	47
Next Steps	56

Purpose of Exam Objectives

When an exam is being developed, the Subject Matter Experts work together to define the role the certified individual will fill. They define all of the tasks and knowledge that an individual would need to have in order to successfully implement the product. This creates the foundation for the objectives and measurement criteria, which are the basis for the certification exam.

The IBM Certification item writers use these objectives to develop the questions that they write and which will appear on the exam.

It is recommended that you review these objectives. Do you know how to complete the task in the objective? Do you know why that task needs to be done? Do you know what will happen if you do it incorrectly? If you are not familiar with a task, then go through the objective and perform that task in your own environment. Read more information on the task. If there is an objective on a task there is about a 95% chance that you WILL see a question about it on the actual exam.

After you have reviewed the objectives and completed your own research, then take the assessment exam. While the assessment exam will not tell you which questions you answered incorrectly, it will tell you how you did by section. This will give you a good indication as to whether you are ready to take the actual exam or if you need to further review the materials.

Note: This is the high-level list of objectives. As you review these objectives, click for a more detailed level of how to perform the task.

High-level Exam Objectives

Section 1 - Cloud Computing Concepts and Benefits	
1.1	Define the cloud computing business advantages.
1.2	Define virtualization as it pertains to cloud computing.
1.3	Define dynamic infrastructure as it pertains to cloud computing.
1.4	Define elasticity as it pertains to cloud computing.
1.5	Define automation as it pertains to cloud computing.
1.6	Define provisioning as it pertains to cloud computing.
1.7	Define why standardization is important to cloud computing.
1.8	Define service catalog as it pertains to cloud computing.
1.9	Define a public cloud.
1.10	Define a private cloud.
1.11	Define a hybrid cloud.
1.12	Define the difference between a private cloud, a public cloud, and a hybrid cloud.
1.13	Define Software as a Service (SaaS).
1.14	Define PaaS.
1.15	Define IaaS.
1.16	Define Database As A Service (DBaaS).
1.17	Explain the benefits of patterns as description of cloud services.
1.18	Position and compare cloud computing to traditional distributed computing technologies such as grid and cluster computing.
1.19	Define software defined environments as they relate to cloud computing.
1.20	Define/summarize how business processes can be automated in a cloud environment.
Section 2 - Cloud Computing Design Principles	
2.1	Define cloud architecture.
2.2	Demonstrate the knowledge of core cloud service models: IaaS, PaaS and SaaS.
2.3	Demonstrate base knowledge needed to advise on creating a cloud infrastructure.
2.4	Explain cloud networking principles.
2.5	Describe the cloud administration interfaces available that can be accessed through Web Services.
2.6	Summarize data and user security strategies in a cloud computing environment.
2.7	Summarize networking performance in a cloud computing environment.
2.8	Identify the role of Web technologies and the importance of Application Programming Interface (API) in cloud computing.
2.9	Define how solutions in the cloud can be more effective (scalability, high availability, service delivery).
2.10	Explain to the customer how some popular billing models work and how they pertain to the software the customer has.

2.11	<u>Define how cloud computing fits in with service management and the Information Technology Infrastructure Library (ITIL) model V3 (ITIL Service Strategy, ITIL Service Design, ITIL Service Transition, ITIL Service Operation, ITIL Continual Service Improvement).</u>
Section 3 - IBM Cloud Computing Architecture	
3.1	<u>Explain the benefits of using the IBM IBM Cloud Computing Reference Architecture (CCRA) V4 Adoption Patterns.</u>
3.2	<u>Explain the Cloud Platform Services Adoption Pattern for CCRA.</u>
3.3	<u>Explain the Cloud Service Provider Adoption Pattern for CCRA.</u>
3.4	<u>Describe the IBM CCRA V4 “Building SaaS” cloud adoption pattern.</u>
3.5	<u>Explain the Cloud Enabled Data Center Adoption Pattern for CCRA.</u>
3.6	<u>Describe the solution integration process detailed in the IBM CCRA V4 to take an existing environment to an IBM Cloud Computing environment.</u>
3.7	<u>Design a secure and reliable cloud computing service model.</u>
3.8	<u>Describe high availability and DR as it pertains to cloud computing.</u>
3.9	<u>Define four defining principles of Cloud computing as presented in the IBM CCRA V4.</u>
3.10	<u>Describe Cloud Service Consumers, Cloud Service Creators, Cloud Service Provider, Cloud Services and the Common Cloud Management Platform.</u>
3.11	<u>Describe how IBM Service Management can effectively manage a customer’s cloud environment.</u>
3.12	<u>Describe the Integration and Extensibility models of cloud solutions described in CCRA V4.</u>
3.13	<u>Understand the role of governance in the CCRA.</u>
3.14	<u>Describe non-functional requirements (NFRs) in the context of a cloud solution.</u>
3.15	<u>Describe the objectives of the Mobile Pattern in the CCRA.</u>
Section 4 - IBM Cloud Computing Solutions	
4.1	<u>Demonstrate understanding of IBM’s cloud offerings for Infrastructure as a Service solutions.</u>
4.2	<u>Describe the management support differences of Platform as a Service offerings between- on and off premise use.</u>
4.3	<u>Describe how IBM Cloud Computing products and solutions can be leveraged to design and provide an effective Software as a Service (SaaS) solution.</u>
4.4	<u>Explain the concept of a Define Database As A Service (DbaaS) and how it relates to a SaaS, IaaS and PaaS or any CCRA adoption pattern in a cloud computing environment.</u>
4.5	<u>Define considerations of storage and data recovery in an IBM Cloud Solution also taking into consideration the different types of storage and how to use them in the different cloud environments.</u>
4.6	<u>Define service orchestration as it pertains to Cloud Computing.</u>

Detailed Exam Objectives

Section 1 - Cloud Computing Concepts and Benefits

1.1. Define the cloud computing business advantages.

SUBTASK(S):

- 1.1.1. Virtualization: Resources can be shared between many computing resources (physical servers or application servers).
 - 1.1.1.1. Provide more efficient utilization of IT resources and reduce hardware cost through resource consolidations and economies-of-scale. Lower total cost of ownership and improving asset utilization.
- 1.1.2. Dynamic: Resources are dynamically provisioned (or deprovisioned) based on consumer demands.
 - 1.1.2.1. Reduce IT cycle time and management cost.
- 1.1.3. Elastic scaling: IT environments scale up and down by any magnitudes as needed to satisfy customer demands.
 - 1.1.3.1. Optimize IT resource utilization and increase flexibility.
- 1.1.4. Service Automation Management: IT environments that provide the capability to request, deliver, and manage IT services automatically.
 - 1.1.4.1. Reduce IT operational costs by automating the processes used to deliver and manage a cloud computing environment.
- 1.1.5. Pervasiveness: Services are delivered through use of Internet and on any platform.
 - 1.1.5.1. Improve customer experience by enabling services to be accessed from anywhere and anytime.
- 1.1.6. Flexible pricing: Services are tracked with usage metrics to enable multiple payment models.
 - 1.1.6.1. Improve cost transparency and offer more flexible pricing schemes.
- 1.1.7. Self-service: Cloud service consumers can initiate workload provisioning on-demand.
 - 1.1.7.1. Improves service delivery by automating the processes used to request workloads.

1.2. Define virtualization as it pertains to cloud computing.

SUBTASK(S):

- 1.2.1. Computing resources (servers, networks, and storage) are dynamically created, expanded, compacted, or moved as demand varies.
- 1.2.2. Under-utilized physical servers are consolidated into a smaller number of more fully utilized physical servers running virtual workloads.
- 1.2.3. Virtualization is a key infrastructure element for cloud computing because:
 - 1.2.3.1. Allows sharing, manageability, and isolation of computing resources.
 - 1.2.3.2. Significant cost savings via server consolidations and optimal resource utilization.
 - 1.2.3.3. Provides a way for provisioning a computing resource dynamically and automatically.

1.3. Define dynamic infrastructure as it pertains to cloud computing.

SUBTASK(S):

1.3.1. Explain dynamic infrastructure:

1.3.1.1. Dynamic infrastructure is an information technology paradigm concerning the design of data centers so that the underlying hardware and software can respond dynamically to changing levels of demand in more fundamental and efficient ways than before.

1.3.2. Explain cloud computing's relationship to dynamic infrastructure.

1.3.2.1. Cloud computing is a way to establish a dynamic infrastructure, specifically to optimize the IT infrastructure through virtualization and self service. This helps to reduce cost, efficiently utilize staff and better manage and automate operations while enabling a data center manager to dynamically adjust their IT infrastructure to meet changing demand levels and new business requirements.

1.4. Define elasticity as it pertains to cloud computing.

SUBTASK(S):

1.4.1. Explain elasticity as it relates to cloud computing.

1.4.1.1. A user can create, launch, and terminate server instances as needed, paying by the hour for active servers, hence the term "elastic".

1.4.1.2. Cloudbursting (capacity over drafting) is automatically adding and subtracting compute and storage capacity on demand to handle workloads in the cloud.

1.4.1.3. Define the 3 levels of elasticity.

1.4.2. Define the impact of elasticity on workloads deployed in the cloud and explain how they interact with cloud management layer to request / relinquish capacity.

1.4.2.1. The cloud computing management platform can detect a workload requires more capacity by either receiving messages over a service bus, or monitoring the infrastructure utilization.

1.4.2.2. The application can receive a signal that additional capacity is now available and scale horizontally.

1.4.2.3. The application can relinquish unutilized capacity and signal the cloud computing management platform to decommission unused capacity.

1.4.3. Explain the difference between elasticity and scalability.

1.4.3.1. Elasticity means the platform and the applications running on the platform can handle sudden, unanticipated, and extraordinary workloads.

1.4.3.2. Scalability is a planned level of capacity, with appropriate overhead that the systems require over time, in addition to the ability to scale in a quick and easy manner.

1.5. Define automation as it pertains to cloud computing.

SUBTASK(S):

Automation is a key infrastructure management for cloud computing because without the benefits of automation, the complexity of a cloud environment is increased significantly and thus generate added costs - costs high enough to cancel out the cost savings derived from cloud computing in the first place.

- 1.5.1. Provides standardization and automation for deployment and management of IT services.
- 1.5.2. Provides the ability to maintain or improve quality and cost per IT service.
- 1.5.3. Provides a management stack that is easier to handle and provides for smoother workload migration.
- 1.5.4. Provides the ability to be audit proof and integrated with process governance.
- 1.5.5. Provides the ability to reduce costly manual interventions.
- 1.5.6. Provides the ability for IT to reduce the skill requirements needed for deploying and managing IT services.
- 1.5.7. Reduces errors caused by manual processes.

1.6. Define provisioning as it pertains to cloud computing.

SUBTASK(S):

- 1.6.1. Provisioning is the automated process of creating, preparing, and configuring computing resources (physical servers, middleware and application server, network, storage space, services, etc.).
- 1.6.2. Provisioning helps optimize availability by maintaining configurations and managing changes to resources.
- 1.6.3. Provisioning is used to capture and rerun scenarios of highly complex tasks, thus minimize the potential for human errors.
- 1.6.4. Explain the trade-offs between provisioning OS image and middleware separately, or with middleware baked into OS image.
 - 1.6.4.1. When middleware and OS image is provisioned separately version control is easier and independent of each other.
 - 1.6.4.2. When middleware is baked with OS image, changes are required to the service catalog every time a version has to be changed.
- 1.6.5. Explain pattern-based provisioning and how it reduces the overall application provisioning time.
 - 1.6.5.1. With pattern-based provisioning multiple software components needed to support a given application are provisioned and integrated in a single logical step.
 - 1.6.5.2. Patterns may also address specific needs such as high availability, security or scalability.
- 1.6.6. Deprovisioning is the automated process of restoring computing resources to their respective resource pools (physical servers, middleware and application server, network, storage space, services, etc.).

1.7. Define why standardization is important to cloud computing.

SUBTASK(S):

- 1.7.1. Consolidating and standardizing the business processes in use in the environment reduce the number of manual actions both physical and electronic required to deploy a service and ensures a consistent process flow is used.
- 1.7.2. A small set of standardized software builds ensure consistency across the cloud environment, encapsulate the best practices for deployment, and reduce the time and effort required to maintain the software builds.
- 1.7.3. Helps maximize repeatability, compatibility, and interoperability. It also drives commoditization and increases quality.

1.8. Define service catalog as it pertains to cloud computing.

SUBTASK(S):

A cloud service catalog:

- 1.8.1. Contains a set of cloud services that an end user can request (usually through a web self-service portal).
- 1.8.2. Acts as the ordering portal for cloud end users, including pricing and service-level commitments and the terms and conditions for service provisioning.
- 1.8.3. Can also be used as a demand management mechanism, directing or incenting customers toward particular services or service configurations or away from legacy or declining services, as well as making sure of alignment with governance and standards through default configurations and service options.
- 1.8.4. Has a self-service look and feel; that is, it provides the ability to select service offerings from the cloud service catalog and generate service requests to have instances of those offerings fulfilled.
- 1.8.5. Is useful in developing suitable cloud-based solutions, thus enabling other IT and business services, which in turn create the value propositions for the investments in cloud architectures.
- 1.8.6. Contains features and characteristics (atomic items that can be configured and preferably priced based upon a "cloud chargeback" mechanism) to fulfill a particular need.
- 1.8.7. Serves as the provisioning interface to automated service fulfillment using a cloud orchestration subsystem.

1.9. Define a public cloud.

SUBTASK(S):

- 1.9.1. Obtaining an instance of cloud computing environment via a public cloud is easy to set-up because hardware, application and bandwidth costs are covered by the provider.
- 1.9.2. The offerings provided in a public cloud environment are 'as is' services.
- 1.9.3. Computing resources in a public cloud can be scaled to meet the needs of the cloud users.
- 1.9.4. Public cloud can use flexible pricing models. Public cloud users do not experience wasted resources because the users pay for what they use on an as-

needed basis, without the requirement to invest in additional internal infrastructure.

- 1.9.5. Public clouds helps businesses shifting the bulk of the costs from capital expenditures and IT infrastructure investment to an operating expense model. It also helps isolate the end users from the complexity of IT operations and management.
- 1.9.6. Public clouds are services offered over an open public network with inherent security considerations.

1.10. Define a private cloud.

SUBTASK(S):

- 1.10.1. A private cloud is either owned by an enterprise or cloud service provider offering either dedicated or shared/multitenant private cloud solutions. The private cloud can only be accessed by internal users. For shared private clouds, isolation of tenants is achieved through customer assigned security zones and dedicated networks.
- 1.10.2. Dedicated private clouds can either be deployed on-premise or off-premise. Shared private clouds are deployed as off-premise or off-premise hybrid (managed-from off-premise, managed-to on premise).
- 1.10.3. A private cloud is operated and maintained by either the enterprise's IT operations or by the cloud service provider.
- 1.10.4. In a private cloud environment, services are delivered and managed through resource management, dynamic allocation, metering and chargeback mechanisms and virtualization.
- 1.10.5. In a private cloud environment the enterprise or cloud service provider governs all computing resources (physical platform, application platform, storage space, applications, services, etc.).
- 1.10.6. In a private cloud environment the enterprise or cloud service provider is responsible for the entire lifecycle and costs of the cloud solution – from service definition, workload allocation, workload management, security, compliance, and service deliver and management.
- 1.10.7. Private clouds are used today for all kinds of workloads, including production but also development and test environments.

1.11. Define a hybrid cloud.

SUBTASK(S):

- 1.11.1. A hybrid cloud model is a composition of two or more cloud types (private and/or public) which are independent but bound together through technologies that enable data and application integration.
- 1.11.2. A hybrid cloud model may enable enterprises to achieve substantial savings in service delivery and service management through the infrastructure and resources provided via the public cloud.

- 1.11.3. A hybrid cloud enables the cloud consumer to segregate workloads based upon security and compliance requirements. For instance, secure data resides on the private cloud and the non-secure data resides on the public cloud.

1.12. Define the difference between a private cloud, a public cloud, and a hybrid cloud.

SUBTASK(S):

1.12.1. Define a private cloud.

In a private cloud, the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

1.12.2. Define a public cloud.

In a public cloud, the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Public clouds are where IT activities/functions are provided as a service over the Internet, which allows access to technology-enabled services without knowledge of, expertise with, or control over the technology infrastructure that supports them.

1.12.3. Define a hybrid cloud.

In a hybrid cloud, the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain independent entities, but are bound together by technology that enables data and application integration (e.g., cloud bursting for load balancing between clouds).

Hybrid clouds are where the external and internal service delivery methods are integrated. Rules and policies are established by the organization based on factors such as security needs, criticality and underlying architecture, so that activities and tasks are allocated to external or internal clouds as appropriate.

1.13. Define Software as a Service (SaaS).

SUBTASK(S):

1.13.1. Explain SaaS.

SaaS capability is provided to the consumer is to use the provider's applications running on a cloud infrastructure². The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

1.13.2. Differentiate SaaS from Platform as a Service (PaaS) and IaaS.

SaaS, PaaS, and IaaS represent different delivery models of a cloud computing environment:

1.13.2.1. SaaS delivers software as a service over the Internet 'as is'.

1.13.2.2. PaaS delivers computing platform and a solution stack as a service.

1.13.2.3. IaaS delivers computer infrastructure as a service.

1.13.3. Provide some examples of SaaS.

1.13.3.1. Google Docs.

1.13.3.2. IBM SmartCloud for Social Business.

1.13.3.3. Salesforce.com.

1.13.3.4. ServiceNow.

1.14. Define PaaS.

SUBTASK(S):

1.14.1. Explain PaaS.

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment

1.14.2. Explain how PaaS related to computing platform.

A computing platform describes some sort of hardware architecture or software framework (including application frameworks), that allows software to run. A PaaS delivers a computing platform as a service.

1.15. Define IaaS.

SUBTASK(S):

1.15.1. Explain IaaS.

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

1.15.2. Explain how IaaS related to utility computing.

Utility computing relates to the business model in which application infrastructure resources, hardware and/or software are delivered. While cloud computing relates to the way we design, build, deploy and run applications that operate in a virtualized environment, sharing resources and boasting the ability to dynamically grow, shrink, and self-heal.

1.15.3. Explain the difference between a private IaaS and a public IaaS.

Private IaaS are deployed, operated and consumed within the boundaries of the internal data center; in this model the IT organization standardizes the set of infrastructural services that it provides and develops the automations to deploy these services rapidly. The consumers of these IaaS services are business lines of development organizations in the enterprise that request these services through a service-catalog. Public IaaS clouds allow to deliver the same set of infrastructural services, but outside of the enterprise boundaries to other companies, to managed accounts, or even to consumer users. Public cloud for delivering IaaS services combine both the IaaS and cloud service provider models.

1.15.4. List some examples of IaaS offerings.

1.15.4.1. Amazon Elastic Compute Cloud.

1.15.4.2. CenturyLink.

1.15.4.3. SoftLayer.

1.16. Define Database As A Service (DBaaS)

SUBTASK(S):

1.16.1. A Database-as-a-Service (**DBaaS**) is a service that is managed by a cloud operator (public or private) that supports applications, without the application team assuming responsibility for traditional database administration functions.

1.16.2. There are two common deployment models: users can run databases on the cloud independently, using a virtual machine image, or they can purchase access to a database service, maintained by a cloud database provider. Of the databases available on the cloud, some are SQL-based and some use a NoSQL data model.

1.16.3. DBaaS use cases: A DBaaS can be used to offset costs of keeping millions of rows of data locally, data archivals, data backup, and data recovery.

1.17. Explain the benefits of patterns as description of cloud services

SUBTASK(S):

1.17.1. Describe the concept of patterns as description for cloud services:

1.17.1.1. Patterns (aka service templates) describe how cloud services and applications are deployed, managed and scaled by an engine supporting the format (domain specific language) of the cloud service.

1.17.1.2. Patterns describe the structure and topology of a cloud service, i.e. the infrastructure and application components, resources and relationships and related management processes required to deliver the cloud service.

1.17.1.3. Pattern components are for instance definition of network and storage elements, image, software binaries, install scripts and recipes.

1.17.1.4. Patterns can either be described in a declarative (e.g. expressed by relationships) or imperative manner (e.g. expressed by a management plan).

- 1.17.1.5. Patterns can be composed out of other templates, e.g. an application pattern may use an infrastructure pattern.
- 1.17.2. Describe the components supporting pattern based deployment:
 - 1.17.2.1. The pattern language (domain specific language) defines the format in which a cloud service is described. There are different formats of patterns available today: standardized, proprietary, open-source and open community formats.
 - 1.17.2.2. Tools like pattern editors support the authoring of patterns.
 - 1.17.2.3. The engine supporting the template language is used to deploy the service template on to a platform (e.g. a private or public cloud, or a specific type of hypervisor).
 - 1.17.2.4. The service template may be published by the provider to a marketplace to make it available to a broader community and others consumers.
- 1.17.3. Describe the benefits of patterns:
 - 1.17.3.1. Patterns codify best practices, promote standardization and reuse, enable faster time-to-value and reduced costs
 - 1.17.3.2. Service templates are portable across different technology platforms supporting the same template language
 - 1.17.3.3. Open standard pattern formats enable ecosystems and avoid vendor lock-in for consumers.

1.18. Position and compare cloud computing to traditional distributed computing technologies such as grid and cluster computing.

SUBTASK(S):

1.18.1. Explain grid computing:

Grid computing is a type of parallel and distributed system that enables the sharing, selection, and aggregation of geographically distributed autonomous resources dynamically at run-time depending on their availability, capability, performance, cost, and users' quality-of-service requirements for solving large-scale compute and data intensive applications such as brain activity analysis, high energy physics etc. Computing grids harness distributed compute power and coordinate the execution of application at internet scale, for the purpose of reducing computation time.

1.18.2. Explain the differences between grid computing and cloud computing:

Grid computing is a form of distributed computing and parallel computing, whereby a 'super and virtual computer' is composed of a cluster of networked, loosely coupled computers acting in concert to perform very large tasks. So the goal of grid computing is to divide a single and large task among many loosely coupled computers. The main difference is that whereas a grid computing is comprised of many computers working together to achieve one goal, cloud computing is aimed to providing computing resource for independent tasks. Moreover, the goal of cloud computing is to provide "any" type of component of the IT stack (infrastructure, platform, applications, and services) on demand.

1.18.3. Explain the relation between grid and cloud computing:

The concept of computing as utility, originally introduced with grid computing is at the core of cloud computing, which has extended such concept to the entire IT stack by leveraging virtualization and introducing economies of scale. Cloud computing resources can be arranged and organized to behave as computing grids, with the added benefit of elastic scalability. Computing grids cannot behave as clouds.

1.18.4. Explain what is a cluster:

A computer cluster is a group of linked computers, working together closely so that in many respects they form a single computer. The components of a cluster are commonly, but not always, connected to each other through fast local area networks.

1.18.5. Highlight differences and similarities between clusters and clouds:

Compute clusters are often based on a Single System Image, whereby the collection of nodes defining the cluster is perceived as single system. This very often implies single root, single file system, single I/O, etc. Moreover, single nodes are designed to be homogeneous in nature, so that the addition of new nodes or replacement of failing ones is effective and almost transparent. A cloud is similar to that as the collection of resources and their topology is often hidden to the user of the cloud. Moreover, aggregations of computing clusters are often at the basis of a cloud computing infrastructure and “virtual computing clusters” can be requested on demand from IaaS providers. While computing clusters primarily addresses the problem of coordinating a collection of co-located nodes to appear as a single powerful computing resource, clouds harnesses a large distributed network of nodes to provide resources on demand.

1.18.6. Identify the key element that set aside cloud computing solutions:

Whereas both computing clusters and grid computing are solutions for harnessing compute power from different resource and offer that as a service. Cloud computing is about virtualizing the entire IT stack (from infrastructure to application services, including computing power) and make it available as a priced utility. Grid and cluster computing primarily address the problem of efficiently executing large computations. Cloud computing is about making any IT resource ubiquitous, accessible from anywhere and anytime.

1.19. Define software defined environments as they relate to cloud computing.

SUBTASK(S):

1.19.1. Software defined environments can be composed of software-defined data center (SDDC), software-defined network (SDN), software-defined compute (SDC) and software-defined storage (SDS).

1.19.1.1. SDDC is a vision for IT infrastructure that extends virtualization concepts such as abstraction, pooling, and automation to all of the data center’s resources and services to achieve IT as a service

1.19.1.2. SDN is an approach to computer networking that allows network administrators to manage network services through abstraction of lower level functionality.

1.19.1.3. SDS is a term for computer data storage technologies which separate storage hardware from the software that manages the storage infrastructure.

Another term out there is software-defined infrastructure (SDI). This refers to the collective of compute, storage and network and the intelligence for managing the infrastructure.

1.19.2. Use of the term software-defined environment (SDE) is the ability to capture information about workloads and the way information is processed, so we can set levels or objectives from a workload perspective, and manage these according to service level agreements (SLAs).

1.19.3. The SDE consumer and SDE providers.

1.19.3.1. An SDE consumer is someone who has a workload they want to deploy and they want to specify policies and non-functional requirements.

1.19.3.2. An SDE provider is a person building an infrastructure to serve these consumers, that could be internal IT, which is moving IT to the Cloud.

1.19.4. OpenStack is a place where vendors come to build a consistent view and see how their products would plug into this API-driven behavioral model of an environment. It is a good framework for getting some consistency in thinking and the approach to doing software-defined everything and can be used as the foundation for a cloud computing environment.

1.20. Define/summarize how business processes can be automated in a cloud environment.

SUBTASK(S):

1.20.1. Describe the existing processes that will be automated as cloud services.

1.20.1.1. Companies that are implementing cloud environment are required to analyze their existing processes to determine the areas where it can be automated in an efficient way when offered as a cloud service.

1.20.1.2. Approvals play an essential role in the core operations of every business. As a rule, most approvals represent the delegation of authority to carry out an activity for example provisioning of computing resources.

1.20.1.3. It is critical to understand and document how approvals are obtained today to see where opportunities for automation and efficiency improvements can be introduced.

1.20.2. Describe how the dynamic provisioning of cloud resources can influence the changes on the business approval process.

1.20.2.1. Customer's existing business approval processes may contain several manual approval steps that may slow down the overall provisioning process. In a cloud environment where IT services are rapidly

provisioned and provided as standardized offerings these manual approval steps should be identified and automated.

1.20.3. Explain the risks of poor or no cloud governance.

1.20.3.1. Poor governance can introduce new risks for security, VM sprawl, and vendor lock-in.

1.20.3.2. Poor governance can result in insufficient capacity as consumers are able to request cloud capacity as they see fit.

1.20.3.3. Poor governance can hinder cloud adoption since there may be a lack of incentive for them to onboard or consume cloud resources.

Section 2 - Cloud Computing Design Principles

2.1. Define cloud architecture.

SUBTASK(S):

- 2.1.1. 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. This cloud model is composed of five essential characteristics, three service models, and four deployment models.
- 2.1.2. Cloud architectures typically leverage Internet-accessible on-demand services. Applications built on cloud architectures are such that the underlying computing infrastructure is used only when it is needed (for example to process a user request), draw the necessary resources on-demand (like compute servers or storage), perform a specific job, then relinquish the resources and often dispose themselves after the job is done. While in operation, the application scales up or down elastically based on resource needs.
- 2.1.3. Characteristics:
 - 2.1.3.1. On demand self service
 - 2.1.3.2. Broad network access
 - 2.1.3.3. Resource pooling
 - 2.1.3.4. Rapid elasticity
 - 2.1.3.5. Measured service

2.2. Demonstrate the knowledge of core cloud service models: IaaS, PaaS and SaaS.

SUBTASK(S):

- 2.2.1. Define cloud computing service models IaaS, PaaS and SaaS

IaaS: In this most basic cloud service model, IaaS providers offer resources including servers, storage and network. The virtual machines are run as guests by a hypervisor, such as Xen or KVM. Pools of hypervisors within the cloud operational support system support large numbers of virtual machines and the ability to scale services up and down according to customers' varying requirements. IaaS clouds often offer additional capabilities such as image management in a virtual image library, raw (block) and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles.

PaaS: In the PaaS model, cloud providers deliver a computing platform typically including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. With some PaaS offers, the underlying computing and storage resources scale automatically to

match application demand such that cloud user does not have to allocate resources manually.

SaaS: In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. The cloud users do not manage the cloud infrastructure and platform on which the application is running. This eliminates the need to install and run the application on the cloud user's own computers simplifying maintenance and support.

2.3. Demonstrate base knowledge needed to advise on creating a cloud infrastructure.

SUBTASK(S):

2.3.1. The creation of a cloud infrastructure requires an environment that needs to address the following areas. A tester must be able to address many of these topics

2.3.1.1. Hardware/platform: A cloud environment needs to select hardware that can run virtualization technology. This includes distributed servers and mainframe solutions with an operating system that supports virtualization software.

2.3.1.2. Virtualization technology such as KVM, VMWare, zVM, etc.

2.3.1.3. Network topologies that supports the virtualization design, WAN/LANs/MPLS, etc., as well as a topology in support of a public, public and/or private cloud.

2.3.1.4. Security framework that meets the requirements of the public, private and private cloud environment at a minimum. If the application(s) that will run on the infrastructure is known, the security requirements can be used to augment that design.

2.3.1.5. Storage and archival needs to manage the data and backup needs

2.3.1.6. Provisioning and orchestration to manage, deploy, spin up, etc., environments

2.3.1.7. Monitoring to provide visibility and management of the environment

2.3.1.8. Capacity, availability and performance topics can be addressed as it relates to creating a cloud infrastructure.

2.4. Explain cloud networking principles.

SUBTASK(S):

2.4.1. Cloud computing networks -- whether they support public, private, or hybrid clouds -- must be able to:

2.4.1.1. Burst up and turn down bandwidth on demand.

2.4.1.2. Provide extremely low latency throughput among storage networks, the data center and the LAN.

2.4.1.3. Allow for non-blocked connections between servers to enable automated movement of virtual machines (VMs).

- 2.4.1.4. Function within a management plane that stretches across enterprise and service provider networks.
- 2.4.1.5. Provide visibility despite this constantly changing environment.
- 2.4.2. Storage plays a major role in cloud computing networks. Applications and data must flow seamlessly among storage systems, the data center and the LAN.
- 2.4.3. In addition to Gigabit Ethernet switches and NIC, network architects and administrators must work with virtual switches and virtual ethernet adapters, which handle switching between VMs and sometimes between physical servers.
- 2.4.4. Very little is static in a cloud environment. Instances of servers and networks are provisioned at the drop of a dime. Automated network processes are essential to provisioning these virtual resources. This means that the network architect must seek out automation tools that handle IP address management, configuration management and resource allocation.

2.5. Describe the cloud administration interfaces available that can be accessed through Web Services.

SUBTASK(S):

- 2.5.1. Select interface providing function required.
 - 2.5.1.1. For customer account, user/group and existing subscription management, select the "Customer Management" interface.
 - 2.5.1.2. For partner account and partner product management, select the "Partner Management" interface.
 - 2.5.1.3. For tasks done by the provider or agents of the provider, select the "Provider Management" Interface.
 - 2.5.1.4. For discovery, selection and ordering of Cloud Services, select the "Storefront" interface.
 - 2.5.1.5. For using Cloud Services, select the "Customer Access" interface.
- 2.5.2. Select technology for interaction (HTTP/HTTPS plus REST and/or SOAP)
 - 2.5.2.1. Based on the choices of interface technology available from the provider and security requirements, use the corresponding client technology.
- 2.5.3. Initiate interaction, including providing authentication credentials.
 - 2.5.3.1. Utilize the protocol interfaces to interact with the system, including providing authentication information corresponding to the provider deployment requirements.

2.6. Summarize data and user security strategies in a cloud computing environment.

SUBTASK(S):

- 2.6.1. Privileged user access: access control measures are required to be employed to protect sensitive data. The following security measures represent general best practice implementations for cloud security.
 - 2.6.1.1. **Implement and maintain a security process.** A security process can provide the structure for managing information security, and the risks and threats to the target environment. In the event of a security breach, the

security process can provide crucial information as to how the cloud is protected, responses to threats, and a line of accountability for management of events.

- 2.6.1.2. **Implement a vulnerability and intrusion management program.** In a trusted cloud environment, you are required to implement a strict vulnerability management program and mechanisms such as intrusion detection systems and intrusion Prevention Systems to ensure that IT resources (servers, network, infrastructure components, and endpoints) are constantly monitored for vulnerabilities and breaches.
- 2.6.1.3. **Build and maintain a secure cloud infrastructure.** A secure infrastructure helps provide cloud resiliency and the confidence that the information stored in the cloud is adequately protected.
- 2.6.1.4. **Ensure confidential data protection.** Data protection is a core principle of information security. All of the prevalent information security regulations and standards, as well as the majority of industry best practices, require that sensitive information be adequately protected in order to preserve confidentiality. Confidentiality of such data is required no matter where that data is resident in the chain of custody, including the cloud environment.
- 2.6.1.5. **Implement strong access and identity management.** Access and identity management are critical to cloud security. They limit access to data and applications to authorized and appropriate users.
- 2.6.1.6. **Establish application and environment provisioning.** In a centrally managed cloud environment, it is essential to have automated provisioning functionality in place.
- 2.6.1.7. **Implement a governance and audit management program.** To be prepared for regulatory or internal audits, you are required to have a program in place that defines when, how, and where to collect log and audit information.
- 2.6.1.8. **Maintain environment testing and validation.** In order to maintain an intact cloud IT environment, you are required to employ different mechanisms for testing and validation.

2.7. Summarize networking performance in a cloud computing environment.

SUBTASK(S):

The data center network must support and enable broader strategic IT initiatives such as server consolidation and virtualization, cloud computing and IT optimization. In this sense, the network must ensure performance, availability, serviceability, and shorten the time required to set up new services. Increasing speed and availability of network bandwidth is creating new opportunities to deliver services across the web and integrate distributed IT resources. Easier access to trusted information and real-time data and analytics will soon become basic expectations.

2.7.1. Capacity and planning:

- 2.7.1.1. Network capacity is defined in two dimensions, vertical and horizontal capacity:
- 2.7.1.2. Vertical capacity relates to the forwarding and processing capacity—in this case, a matrix such as bandwidth, packet rate, concurrent sessions, and so on.
- 2.7.1.3. Horizontal capacity involves the breadth and reach of the network—in this case, a matrix such as server port counts, external connectivity bandwidth, and so on.
- 2.7.2. Describe the network performance implications of building data center clouds.
 - 2.7.2.1. Data center clouds are formed by connecting two or more data center cloud networks over a wide area network (WAN). Due to the inherent nature of WANs, network data loss and latency must be closely examined to make sure that sufficient bandwidth is allocated.
- 2.7.3. Identify the network performance issues related to creating multi-network data centers.
 - 2.7.3.1. The latency accumulated in networks largely in proportion to the number of interfaces a packet transits from source to destination, and each switch that handles packets poses risk of loss and delay. Network should be planned as flat as possible.
- 2.7.4. Layer 2 network requirements:
 - 2.7.4.1. The widespread adoption of server virtualization technologies drives a significant expansion of the Layer 2 domain, and also brings the need to extend Layer 2 domains across physically separated data centers in order to stretch VLANs to enable VM mobility by using technologies such as VMware, VMotion, or POWER Live Partition Mobility. These are very challenging requirements to satisfy in order to achieve the service delivery objectives since they directly impact the scalability (in terms of new MAC addresses that can be included in a Layer 2 domain) and flexibility (in terms of the time and effort needed to deploy new services) of the data center network.
- 2.7.5. Control Plane Stability:
 - 2.7.5.1. The stability of the control plane in a typical Layer 2 data center network is typically controlled by spanning tree protocol (STP) or one of its many variants. This approach, however, does not have the robustness, flexibility and efficiency that are required to assure service delivery to the business. For example, the typical convergence time required to recover from a link failure is not in synch with the needs of today's network-dependent and high-paced business environment. This limitation hence has a huge impact on the availability and reliability of the data center network.
- 2.7.6. Optimal Use of Network Resources:
 - 2.7.6.1. Another drawback of STP is that in order to avoid loops in a Layer 2 network, a tree topology must be enforced by disabling a subset of the available links. So usually 50% of the available links are idle and the efficiency of the capacity usage is suboptimal at best. This can be mitigated by balancing the available VLANs across different STP

instances, but it goes without saying that being able to exploit 100% of the available capacity would be a huge improvement from a data center network performance point of view.

2.7.7. Optimal Use of Network Awareness:

2.7.7.1. Virtual machines are the new building block in the data center and the importance of physical NICs for the network architecture fades when compared to the virtual networking realm inside the server platforms. On the other hand, it is difficult to manage both the virtual and the physical network environment with a consistent set of tools and orchestrate changes in an end-to-end fashion. This trend puts a lot of pressure on the serviceability and manageability of the data center network and can also impact its availability if changes are not agreed across different functional teams in charge of the infrastructure management.

2.7.8. End-to-end network visibility:

2.7.8.1. Server consolidation and virtualization initiatives demand more bandwidth per physical machine and the same is true on a WAN scale when consolidating scattered data centers into fewer ones. This and the fact that it is very difficult to obtain end-to-end visibility of the network flows (different teams in charge of managing virtual resources inside servers, Blade switches, LAN switches, and WAN routers) have the risky consequence that it is becoming increasingly more difficult to spot and remove network bottlenecks in a timely and seamless fashion. Clearly this has a significant impact on the performance and even the availability of the enterprise network if the quality of service (QoS) model is not designed and enforced properly.

2.8. Identify the role of Web technologies and the importance of Application Programming Interface (API) in cloud computing.

SUBTASK(S):

2.8.1. Identify the Internet, and more generally Internet-based protocols define the channels through which cloud computing services are made available and delivered. Highlight the Web as the primary interface to deliver such a service.

2.8.2. Focus on the concept of API as a generic abstraction through which access cloud services.

2.8.3. Describe how existing Web service technologies and API can be used by cloud providers to offer cloud services.

2.8.3.1. Cloud service providers use existing Web technologies such as PHP, AJAX, REST API, SOAP, XML HTML5 and others to develop a dynamic Web front-end for its end-users to see and order their cloud service offerings.

2.8.4. Describe how Web technologies and API can be used by end-users to access cloud services.

2.8.4.1. In a SaaS model, users will only be required to access to the applications that are being offered as opposed to the infrastructure platform that the application is running on. Generally, these applications are provided in

the form of a Web application. In some cases, cloud service providers offer wrapper Web service APIs that give its users the ability to integrate with other applications on the Web.

- 2.8.5. Identify some of the common Web services that are offered by cloud service providers.
 - 2.8.5.1. Cloud services providers offer web services that offer access to: storage, computing, messaging, data, and other cloud services.
- 2.8.6. Discuss cloud application development as a result of service composition and integration through the APIs that these services expose.

2.9. Define how solutions in the cloud can be more effective (scalability, high availability, service delivery).

SUBTASK(S):

The following factors will affect the performance of a cloud-based solution:

- 2.9.1. Software & Service Delivery:
 - 2.9.1.1. Response time.
 - 2.9.1.2. System management & maintenance planning.
 - 2.9.1.3. Proactive communications.
 - 2.9.1.4. Notifications regarding maintenance activities.
 - 2.9.1.5. System monitoring.
 - 2.9.1.6. Key Performance Indicators.
- 2.9.2. System Scalability:
 - 2.9.2.1. Ability to respond to large volumes of service requests & users.
 - 2.9.2.2. Ability to handle high volumes of services during peak demands.
 - 2.9.2.3. Ability for system expansion with minimal costs.
 - 2.9.2.4. Consistent service quality.
 - 2.9.2.5. Consistent service and system performance.
 - 2.9.2.6. Reliability as service request volumes grow.
- 2.9.3. High Availability and Disaster Recovery:
 - 2.9.3.1. Facilities with reliable power, cooling, and network infrastructure.
 - 2.9.3.2. High-availability infrastructure, including networking, server infrastructure, and software.
 - 2.9.3.3. Resource redundancy (eg. compute clustering, redundant network).
 - 2.9.3.4. Operational availability capability (based upon service level agreements (SLAs)).

2.10. Explain to the customer how some popular billing models work and how they pertain to the software the customer has.

SUBTASK(S):

- 2.10.1. Subscription-based pricing: In this model customer pay to have access to the product/service for a period of time – typically on a monthly basis. The model was pioneered by magazines and newspapers, but is now used by many businesses and Websites. Rather than selling products individually, a subscription sells periodic (monthly or yearly or seasonal) use or access to a

product or service. The model typically allows for unlimited usage during the subscription period. So that the customer pays the same amount regardless of the amount of resources they used.

- 2.10.2. Elastic pricing or Consumption-based pricing model: In this model the cost is tied to what customer actually use. Under these models you only pay for the amount of resources/services you actually use such as service functions, disk space, CPU time and network traffic.
- 2.10.3. Market-based pricing or Spot pricing for cloud: With market-based pricing there is a market price for a service, the market price varies over time based on supply and demand. Market forces govern the spot-pricing model i.e., when computing and storage resources are in high demand, the spot market will drive the price of services higher. Conversely, when resources are in low demand, the spot market will drive the price lower offering opportunities for bargain hunters. On the other side as a customer you can buy the service at the current price and use it straight away. Or you can make a bid to use the service at a lower price and if the market price reaches your price then your workload will be activated and you will be charged at your bid price.
- 2.10.4. Cloud chargeback/showback: In this model the consumer pay for the usage. It correlates utilization back to cloud consumers or corporate departments, so that usage can be charged if desired.

2.11. Define how cloud computing fits in with service management and the Information Technology Infrastructure Library (ITIL) model V3 (ITIL Service Strategy, ITIL Service Design, ITIL Service Transition, ITIL Service Operation, ITIL Continual Service Improvement).

SUBTASK(S):

- 2.11.1. Explain how ITIL service strategy pertains to cloud computing.
 - 2.11.1.1. ITIL service strategy provides guidance on clarification and prioritization of service provider investments in services. It focuses on helping business improve and develop over the long term, based upon a market-driven approach. Key topics covered include service value definition, business case development, market analysis, and service provider types.
 - 2.11.1.2. The market dynamics and business objectives are essentially same in a cloud computing model. The differences would be in the sourcing, packaging and bundling of services, and how service users are charged for the utilization of services.
 - 2.11.1.3. The service portfolio, which decides on a strategy to serve customers and to develop the service provider's offerings and capabilities, will include the cloud services.
- 2.11.2. Explain how ITIL service design pertains to cloud computing.
 - 2.11.2.1. ITIL service design provides good practice guidance on the design of IT services, processes, and other aspects of the service management effort. Its scope includes the design of new services, as well as changes and improvements to existing ones.

- 2.11.2.2. ITIL service design encompasses all elements relevant to technology service delivery, rather than focusing solely on design of the technology itself. As such, service design addresses how a planned service solution interacts with business and technical environments, service management systems required to support the service, processes which interact with the service, technology, and architecture required to support the service, and the supply chain required to support the planned service.
- 2.11.2.3. Service design must also be implemented with cloud computing characteristics in mind, including:
 - 2.11.2.3.1. Service level agreements will pertain to virtual assets, which are dependent on the physical infrastructure on which the virtual assets are located.
 - 2.11.2.3.2. Capacity management requires that physical infrastructure as well as the virtual asset be considered.
 - 2.11.2.3.2.1. The capabilities of cloud computing provide tools to further service continuity and availability.
 - 2.11.2.3.2.2. Auditing mechanisms for virtual assets must exist to consider usage of virtual assets, and measure how that correlates to use of a given physical asset.
- 2.11.3. Explain how ITIL service transition pertains to cloud computing.
 - 2.11.3.1. ITIL service transition relates to the delivery of services required by a business into an operational usage state. It provides guidance on transferring the control of services between customers and service providers.
 - 2.11.3.2. ITIL service transition provides guidance on managing the complexity of changes to services and service management processes in a coordinated manner.
 - 2.11.3.3. Cloud computing provides an especially fluid environment, so Change and Configuration management are both important and challenging. (example: How to track a virtual machine)
 - 2.11.3.4. The virtual machine may be started up, shut off, cloned, modified, destroyed and recreated.
 - 2.11.3.5. As a configuration item, service requests for provision and modification of virtual assets must follow a process which maintains control while matching the flexibility of virtual assets in the cloud. Incident and problem management must also reflect the specific challenges of virtual assets.
 - 2.11.3.6. Release management must encompass issues regarding the ability to not only clone virtual assets, but then modify and redeploy those assets (as an example, how will the upgrade of the operating system on a virtual server propagate to clones of that virtual server, some of which may have been modified).
- 2.11.4. Explain how ITIL service operation pertains to cloud computing.

- 2.11.4.1. ITIL service operation is the part of the lifecycle where the services and value are actually directly delivered. The monitoring of problems and balance between service reliability and cost etc. are considered.
- 2.11.4.2. The functions include technical management, application management, operations management and service desk as well as, responsibilities for staff engaging in service operation.
- 2.11.4.3. ITIL service operation aims to make sure that IT services are delivered effectively and efficiently. This includes fulfilling user requests, resolving service failures, fixing problems, as well as carrying out routine operational tasks.
- 2.11.4.4. Monitoring for the availability of IT services and security compliance will pose increased challenges when services are hosted in vendor cloud environments.
- 2.11.5. Explain how ITIL continual service improvement pertains to cloud computing.
 - 2.11.5.1. ITIL continual service improvement aims to align and realign IT services to changing business needs by identifying and implementing improvements to the IT services that support the business processes.
 - 2.11.5.2. The ITIL continual service improvement process aims to use methods from quality management in order to learn from past successes and failures. The CSI process implements a closed-loop feedback system as specified in ISO 20000 as a means to continually improve the effectiveness and efficiency of IT services and processes.
- 2.11.6. Explain challenges in using the ITIL methodology with cloud computing. Challenges include:
 - 2.11.6.1. The flexibility and increasingly dynamic nature of a cloud environment;
 - 2.11.6.2. License management concerns (example: managing software licenses) for virtual assets;
 - 2.11.6.3. The separation of physical infrastructure from the services provided by virtual assets that run on that infrastructure.
- 2.11.7. Explain the benefits of using a ITIL methodology with cloud computing
 - 2.11.7.1. Cloud computing can assist with many areas of ITIL methodology implementation. (example: using the ability to migrate virtual assets to meet SLAs and more effectively perform capacity management)
 - 2.11.7.2. Likewise, the fluid nature of a cloud computing environment can benefit a formal management methodology such as ITIL.
 - 2.11.7.3. Extending service delivery with Enterprise Service Management (integrated with ITIL process guidelines), which allows to completely integrated the cloud world with the remaining part of the enterprise by including the cloud infrastructure and services in the enterprise ITIL process guidelines.

Section 3 - IBM Cloud Computing Architecture

3.1. Explain the benefits of using the IBM IBM Cloud Computing Reference Architecture (CCRA) V4 Adoption Patterns.

SUBTASK(S):

3.1.1. Adoption Pattern – A collection of commonly observed functions and features that customers desire in their solution. Where a customer starts to solve a specific business problem, typically driven by the same business motivation. e.g. “Drive down IT costs by improving delivery time and quality, and lowering risks associated with delivery of new IT environments to business and software application development and delivery.”

3.1.1.1. CCRA categorize the cloud business models and corresponding architecture by the following “cloud adoption patterns” :

3.1.1.1.1. Cloud Enabled Data Center (IaaS): Cloud Enabled Data Center (CeDC) is one of the six «cloud adoption patterns» that are described in the IBM Cloud Computing Reference Architecture (CCRA). It provides guidance on how to build a private cloud for the delivery of IaaS services. CeDC solution is described through four «architectural patterns» called macro-patterns, where each macro-pattern

3.1.1.1.2. Platform-as-a-Service (PaaS): To gain faster time to market in building and deploying applications with standardized, automated, pre-integrated, open standards based infrastructure tuned to application specific needs. Also it provides the blueprint to customers for defining private and public cloud platforms plus the associated services.

3.1.1.1.3. Software-as-a-Service (SaaS): Building SaaS cloud adoption pattern describes the IBM recommended solution for building a SaaS cloud solution. For each phase of a client engagement (or cloud sales cycle) a set of deliverables is provided that described in details all the aspects for that phase (e.g. business drivers, use-cases, architectural decisions, architecture overview, etc..). This approach allows both the sales representatives and architects to use the pattern for proposing and designing a SaaS cloud solution

3.1.1.1.4. Cloud Service Providers (CSP2 –Building Commercial XaaS –): Deliver innovative business Models as a Cloud Services Provider, Service provider is an encapsulation of IaaS , PaaS , SaaS

3.1.1.1.5. Mobile

3.1.1.1.6. Analytics

3.2. Explain the Cloud Platform Services Adoption Pattern for CCRA.

SUBTASK(S):

- 3.2.1. Describe the roles – Consumer (Customer, Partner, Agent), Creator, Provider and Broker
 - 3.2.1.1. Consumer represents any person or system that can interact with the cloud computing environment, including customer, partner, developer and provider employees.
 - 3.2.1.2. Creators create the applications, packaging and definitions that become the Cloud Services offered by the provider.
 - 3.2.1.3. Provider is the entity that makes the cloud services available and manages the support systems that manage the cloud services.
 - 3.2.1.4. Broker is the entity to through API the user and the provider.
- 3.2.2. Describe the domains within the Provider – Access, Cloud Services, Common Cloud Management Platform (BSS, OSS), Infrastructure.
 - 3.2.2.1. The Access domain provides the edge of network infrastructure for the Provider including security, routing, network optimization and network protection functions
- 3.2.3. Describe the functional categories within Business Support Services (BSS).
 - 3.2.3.1. BSS categories are Customer Management, Product Management, Partner Management, Subscription Management, Metering, Billing, Rating and Charging, Financial Management, Analytics and Reporting
- 3.2.4. Describe the functional categories within Operational Support Services (OSS).
 - 3.2.4.1. OSS categories are Service Automation, Package On-boarding, Service Quality Management, Package Management, Service Operations Management, VM Management and Resource Management
- 3.2.5. Describe the five access interfaces – Customer Access, Storefront, Customer Management, Partner Management, and Provider Management.
 - 3.2.5.1. Customer Access provides the interface (visual or non-visual) for interacting with Cloud Services.
 - 3.2.5.2. Storefront provides the interface for discovering, selecting and ordering Cloud Services.
 - 3.2.5.3. Customer Management provides the interface for managing customer accounts, users/groups and existing subscriptions.
 - 3.2.5.4. Partner Management provides the interface for managing partner accounts and product management by partners.
 - 3.2.5.5. Provider Management provides the interfaces for managing the cloud and its systems by the provider and its agents.
- 3.2.6. Describe the aggregated patterns provided by the Platform Services.
 - 3.2.6.1. The Platform Services adoption pattern describes methods to provide application development and deployment environments, middleware deployment and management environments, and cloud integration services where the consumer has access to the data and applications for the platform, but not the underlying supporting infrastructure.
 - 3.2.6.2. Application Lifecycle Management (ALM) - this pattern covers the continuum of managing an application through governance, development, and maintenance. Includes Analyze, On-Board, Develop, Test, Continuous Deployment, and Manage. Focus areas: Continuous delivery and DevOps.

- 3.2.6.3. Middleware deployment and management (Elastic Services and Applications Platform - ESAP) - this pattern covers the ability to increase or decrease capacity dynamically to provide latency optimization and redundancy for scalable and fault-tolerant applications and database infrastructure deployable in a single VM or a cluster. Deployment of middleware and applications including for example data and applications like SAP. Focus areas: Deployment of cloud enabled or cloud born applications; elasticity and resiliency services; elastic data caching; and scale-out data (NoSQL) and scale-up data.
- 3.2.6.4. Cloud Services and Operating Environment (CSOE) - this pattern covers the APIs for various cloud integrations including Private to Private, Private to Public, Private to On-Premise, Public to On-Premise, Public to Public, and Public to Private Clouds. Includes “Born on the Cloud” and SaaS solutions. Focus areas: Hybrid Cloud, API management, Private/Public PaaS integration, Platform linkage up to SaaS and down to IaaS.

3.3. Explain the Cloud Service Provider Adoption Pattern for CCRA.

SUBTASK(S):

- 3.3.1. Simple CSP Services - Provides deployment, automation, security, customer management, metering and billing services that allow to delivery IaaS/PaaS services in a simple, repeatable and secure way to end-users inside or outside the enterprise boundaries and to account them for these services use
- 3.3.2. Advanced CSP Services - Provides an highly customizable storefront that includes the most typical e-commerce features like shopping-kart, credit-card-payment, etc.. and that allows a cloud service provider to sell its own services or to resell, white-label or broker third –party cloud services to consumer users
- 3.3.3. Describe the roles – Consumer (Customer, Partner, Agent), Creator and Provider.
 - 3.3.3.1. Consumer represents any person or system that can interact with the Cloud Computing environment, including customer, partner, developer and provider employees.
 - 3.3.3.2. Creators create the applications, packaging and definitions that become the Cloud Services offered by the provider.
 - 3.3.3.3. Provider is the entity that makes the Cloud Services available and manages the support systems that manage the Cloud Services.
- 3.3.4. List the solutions and products that implement the adoption pattern
 - 3.3.4.1. The service provider adoption pattern provides a core infrastructure management solution, and a storefront/aggregation solution. The two may be delivered together or independently. For complex IaaS environments, the IBM SmartCloud Aggregation for Service Providers is combined with a custom delivered CCRA Cloud Enabled Data Center deployment.
 - 3.3.4.2. Solution: IBM SmartCloud Integrated Infrastructure for service providers.

- 3.3.4.2.1. IBM SmartCloud Provisioning, IBM SmartCloud Monitoring, IBM SmartCloud Cost Management
- 3.3.4.3. Solution: IBM SmartCloud Aggregation for Service Providers
 - 3.3.4.3.1. IBM WebSphere Cast Iron, IBM Cloud Services Aggregation Pack
 - 3.3.4.3.2. Describe general ecosystem to deliver all services to service provider

3.4. Describe the IBM CCRA V4 “Building SaaS” cloud adoption pattern.

SUBTASK(S):

Describe the main concepts of IBM CCRA V4 “Building SaaS” adoption pattern

3.4.1. **Architectural principles of IBM CCRA V4 and SaaS adoption pattern:**

- 3.4.1.1. SaaS objectives – Building SaaS cloud adoption pattern describes the IBM recommended solution for building a SaaS cloud solution.

3.4.2. **SaaS general overview :**

- 3.4.2.1. Major SaaS concepts - describes the major characteristics of SaaS solutions including provider/consumers roles, security and MultiTenancy aspects, pricing, billing and payment processes and subscription management.

- 3.4.2.2. SaaS delivery models- Describes the main delivery models for SaaS solutions that can be:

Primary hybrid is a method of extending on-premise or hosted deployments into a cloud environment. Batch processing and data mining are two key examples of primary hybrid deployment because they may not be required for run-time services and may inject data into the offering at selected points.

Hybrid clouds involve attaching one or more on-premise or hosted environments to a true IaaS or PaaS environment. Hybrid clouds are a mixed resource environment, combining both local and cloud resources to provide a SaaS service and rely on both environments to deliver true end-to-end functionality.

Full cloud SaaS solution involves delivering a production-ready solution using only cloud services from one or more cloud providers. All functional aspects of a full cloud solution used to deliver the client-visible service reside completely within the cloud. Non-production facing elements such as development and testing may use a hybrid cloud or a fully on-premise solution

Extended cloud scenario is a simple extension of the full cloud. A provider who chooses to use more than one cloud data center and to link or decouple services may extend

3.4.3. **Client requirements for building SaaS solutions.**

- 3.4.3.1. Business drivers – defines the typical business drivers that drive our clients to build SaaS solutions; same samples are:

- 3.4.3.1.1. Implement a more competitive and business and licensing model.

- 3.4.3.1.2. allow for easy consumption of services.
 - 3.4.3.1.3. reduce complexity due to S/W installation and reduces TCP.
 - 3.4.3.1.4. Etc ...
 - 3.4.3.2. User roles – Describe the three major roles of cloud SaaS solutions that are SaaS Vendor Role, SaaS Provider role and SaaS Consumer role.
 - 3.4.3.3. Use cases – Defines all the typical use-cases of cloud SaaS solutions. The major use-case packages that have been identified for SaaS solutions are:
 - 3.4.3.3.1. Subscription Management: Create and manage customer accounts and identities (tenants).
 - 3.4.3.3.2. Security Management.
 - 3.4.3.3.3. Licensing.
 - 3.4.3.3.4. Service Extensions to Link on-premise applications and authentication securely to external SaaS service.
 - 3.4.3.3.5. External Usage to create service offerings that can be reused by other offerings in an automated fashion.
 - 3.4.3.3.6. Charging/Billing/Accounting.
 - 3.4.3.3.7. Backup/Resiliency.
 - 3.4.3.3.8. Import/Export of tenant information for data onboarding, DR, etc.
 - 3.4.3.4. Non-functional requirements – the typical NFRs for SaaS solutions are in the areas of reliability, availability, security, performances and scalability.
- 3.4.4. **Design of SaaS solutions:**
 - 3.4.4.1. SaaS Components model – Describes the major logical components that allow to build a SaaS solution; the major logical components for SaaS solutions are:
 - 3.4.4.1.1. Base cloud infrastructure (can based on private infrastructure of from public IaaS or PaaS clouds)
 - 3.4.4.1.2. Load Balancers
 - 3.4.4.1.3. Multi-Tenancy Injection and Control
 - 3.4.4.1.4. Integration Control
 - 3.4.4.1.5. Service Management and Monitoring
 - 3.4.4.1.6. Data backup and recovery
 - 3.4.4.1.7. Shared Services components (e.g. Database as a Service (DBaaS))
 - 3.4.4.1.8. Identity and Access management
 - 3.4.4.1.9. Security and application development
 - 3.4.4.2. SaaS Architecture Overview – Describes the architecture that realizes a SaaS solution and how the above components map to the corresponding IBM (and non-IBM) products that realize them.
 - 3.4.4.2.1. Base Cloud Infrastructure – Recommendation is for IBM SCE
 - 3.4.4.2.2. Load Balancers – HA Proxy Servers, F5 or LBaaS from SCE (when it will be available)
 - 3.4.4.2.3. Multi-Tenancy Injection and Control – Corent Multi-Tenant Server and SaaS Cockpit
 - 3.4.4.2.4. Integration Control – CastIron Live

- 3.4.4.2.5. Service Management and Monitoring - SL Corporation (for use with pureScale/SCE) , 2020 Project (for log analytics), Tracelytics (for Performance Analytics)
- 3.4.4.2.6. Data backup and recovery – Asigra (Data Backup as a service), Sonian (Data Archival as a Service)
- 3.4.4.2.7. Shared Services components (e.g. DBaaS) – DB2, MongoDB
- 3.4.4.2.8. Identity and Access management – TDS, TDI, TIM, TAMEB, TFIM
- 3.4.4.2.9. Security and application development – IBM Rational AppScan
- 3.4.4.3. SaaS Architectural decisions – When designing SaaS solutions the following architectural decisions must be taken:
 - 3.4.4.3.1. Integration Management.
 - 3.4.4.3.2. Security and Privacy Management.
 - 3.4.4.3.3. Users management.
 - 3.4.4.3.4. Data load, Data Management and Data resiliency.
 - 3.4.4.3.5. Service and performance monitoring and management.
- 3.4.5. **Implementation of SaaS solutions**
 - 3.4.5.1. SaaS Operational models – Describe the most common way the deploy the components that implement a SaaS solution.

3.5. Explain the Cloud Enabled Data Center Adoption Pattern for CCRA.

SUBTASK(S):

- 3.5.1. Describe the purpose of the CeDC adoption pattern
 - 3.5.1.1. Provides a prescriptive guidance to build Private Clouds for IaaS, starting from a simple entry implementation up to a comprehensive infrastructure that provides fully ITIL managed cloud services.
 - 3.5.1.2. Describes different implementation models for building a private cloud for IaaS leveraging on-premise or of-premise infrastructure.
 - 3.5.1.3. Reuse knowledge of hundreds of successful cloud projects
- 3.5.2. Describe the levels of maturity as given by the cloud enabled data center maturity model
 - 3.5.2.1. Virtualized (maturity level 1):
 - 3.5.2.1.1. Many organizations are at this level today, and use virtualization to manage storage, network or compute. However at this level there is still very little automation to support virtualization.
 - 3.5.2.2. Deployed (maturity level 2):
 - 3.5.2.2.1. At the deployed level, the virtualization technologies are augmented with an automation layer. Basic management processes are established to track costs.
 - 3.5.2.3. Optimized (maturity level 3):
 - 3.5.2.3.1. At this level an organization incorporates additional capabilities to manage the infrastructure in order to reduce the

operational costs and improves the service level agreements (SLAs) and quality of service.

- 3.5.2.4. Enhanced (maturity level 4):
 - 3.5.2.4.1. With level 4 the focus shifts to high value services such as, provisioning of application topologies, disaster recovery(DR) of cloud environment, and cloud-based backup services.
 - 3.5.2.4.2. Level 4 provides organizations the ability to orchestrate provisioning of services across data centers and provisioning to off-premise public clouds to dynamically scale out and handle peak loads.
- 3.5.2.5. Monetized (maturity level 5):
 - 3.5.2.5.1. At this level, IT organization contribute to generate revenue by offering a utility service for obtaining compute and storage to other organizations or companies or to consumers or users.
 - 3.5.2.5.2. At this level vigorous processes are in place for service inception, development, offering, billing, and retirement and a greater focus on the ease of use and customizability of user interfaces.
 - 3.5.2.5.3. This level represents the natural evolution toward a Cloud Service Provider business model.
- 3.5.3. Describe the user roles to support the cloud enabled data center solution:
 - 3.5.3.1. Cloud Service Creator: Develop the technical as well as the business aspects of a (simple or higher-level) cloud service offering.
 - 3.5.3.2. Cloud Service Provider: Provide all types of services to a Service Consumer.
 - 3.5.3.3. Cloud Service Consumer: Consumes all types of services offered by a Service Provider.
- 3.5.4. Describe the four major of areas of cloud enabled data center use cases, called macro patterns:
 - 3.5.4.1. Simple IaaS - Start to embrace the cloud model by delivering simple VMs via service-catalog
 - 3.5.4.1.1. This is the entry point into the cloud space.
 - 3.5.4.1.2. Customer wants to start building a multi-tenant cloud infrastructure to deliver simple VMs (configured with proper network and storage) that covers 70 % of requests from business lines.
 - 3.5.4.2. Managed IaaS - Manage the cloud infrastructure to increase SLA/QoS, security and reliability.
 - 3.5.4.2.1. Customers wants to complement the first macro-pattern by adding management capabilities that allow to manage aspects like SLAs, security, resiliency, capacity planning, etc... for both the infrastructure that provides the cloud and the cloud service itself.
 - 3.5.4.3. Advanced IaaS - Deliver more sophisticated and composite cloud services.

- 3.5.4.3.1. Customers wants to deliver more sophisticated cloud services like the ones that are typically required in production environments.
- 3.5.4.3.2. Such services goes beyond the simple deployment of VMs, but require to orchestrate the provisioning and configuration of compute, storage and network resources.
- 3.5.4.3.3. Such production-like services typically require most of the management capabilities provided by the “Managed IaaS” services in place to manage the service itself and guarantee the requested SLAs.
- 3.5.4.4. ITIL process integrated IaaS - Integrate IaaS with the existing enterprise ITIL processes.
 - 3.5.4.4.1. Customers want to completely integrate the cloud world with the remaining part of the enterprise by including the cloud infrastructure and services in the enterprise ITIL processes.
- 3.5.5. Describe the cloud enabled data center implementation models:
 - 3.5.5.1. On-premise-hybrid: Classic CeDC model where the cloud management infrastructure is built on-premise and it manages and allocates resources mainly on-premise with some extension to off-premise resources. Resources can be allocated into the off-premise environment to address the usage peaks (the so called cloud-bursting scenario) or to provision non-critical workloads like for example dev & test environments
 - 3.5.5.2. Off-premise-hybrid: In this CeDC model the cloud management stack resides in the off-premise environment and manages resources that can be either off-premise or on-premise or both. This model allows to offload the burden of having a cloud management-environment in-house, it allows to leverage off-premise resources to allocate non-critical workloads but it still allows to allocate your critical workloads on-premise (for security and performance reasons) or to efficiently access System-of-records resources (typically data) on-premise.
 - 3.5.5.3. Full off-premise: In this CeDC model, all the cloud management and managed environments reside off-premise. This model can be used to allocate through a cloud-delivery model some specific workloads (like for example dev&test environments, or simulation applications) into an off-premise environment so that customer can leverage the elasticity of the off-premise environment. This model can also be used to build cloud service providers solutions.

3.6. Describe the solution integration process detailed in the IBM CCRA V4 to take an existing environment to an IBM Cloud Computing environment.

SUBTASK(S):

- 3.6.1. Consolidate IT Resources into a single pool.
- 3.6.2. Virtualize IT resources so that they function as a single resource to consolidate and optimize their computing capacity.

- 3.6.3. Standardize platforms so that resources, applications and hardware assemblies can be moved from one deployment system to another.
- 3.6.4. Automate workloads to enable consistent and rapid service delivery.
- 3.6.5. Migrating workloads to a cloud environment to enable users to select from a service catalog allowing selectable workload characteristics like computing capacity, storage class and applications, as well as parameters for usage.
- 3.6.6. Train users on accessing resources on the newly deployed cloud.

3.7. Design a secure and reliable cloud computing service model.

SUBTASK(S):

- 3.7.1. BPaaS: It is any type of horizontal or vertical business process that's delivered based on the cloud services model.
 - 3.7.1.1. The following characteristics define BPaaS:
 - 3.7.1.1.1. The BPaaS sits on top of the other three foundational cloud services: SaaS, PaaS, and IaaS.
 - 3.7.1.1.2. A BPaaS service is configurable based on the process being designed.
 - 3.7.1.1.3. A BPaaS service must have well-defined APIs so it can be easily connected to related services.
 - 3.7.1.1.4. A BPaaS must be able to support multiple languages and multiple deployment environments because a business cannot predict how a business process will be leveraged in the future.
 - 3.7.1.2. The scenario for sharing the BPM middleware is as follows:
 - 3.7.1.2.1. A tenant is defined as a team of users that wants to collaborate and develop their business processes. In an enterprise environment, this may map to a business unit, or a team inside a business unit.
 - 3.7.1.2.2. A tenant is on-boarded to the system via some form of a self-service portal that provides tenant management. After the tenant is on-boarded, the users from the tenant can start authoring and testing processes in the shared IBM Business Process Manager Process Designer and Process Center. Their processes will not be visible to other users from other tenants.
 - 3.7.1.2.3. A dedicated Process Server is provisioned for each tenant and is connected to the shared Process Center. Only users from the tenant can deploy, run and monitor processes on the Process Server dedicated to the tenant. This can be clustered to meet the different SLA requirements for each tenant.
- 3.7.2. **Explain the security considerations for Common Cloud Management Platform (CCMP), Hardware Infrastructure and Cloud Services:**
 - 3.7.2.1. Non-functional aspects such as security, spanning the CCMP, Hardware infrastructure and Cloud Services must be viewed from an end-to-end perspective including the structure of CCMP by itself, the way the hardware infrastructure is set up (e.g. in terms of isolation, network

zoning setup, data center setup for DR etc.) and how the cloud services are implemented.

3.7.3. Examples for security considerations:

3.7.3.1. Some of the examples of security considerations as mentioned in the IBM's CCRA are:

- 3.7.3.1.1. Security Event Management.
- 3.7.3.1.2. Security Policy.
- 3.7.3.1.3. Threat & Vulnerability Management.
- 3.7.3.1.4. Software, System & Service Assurance.
- 3.7.3.1.5. Data and Information Protection.
- 3.7.3.1.6. Security Entitlement.
- 3.7.3.1.7. Access & Identity Lifecycle Management.
- 3.7.3.1.8. Compliance.
- 3.7.3.1.9. Data Policy Enforcement.

3.7.4. Clients' security objectives reflect their responsibilities when adopting Cloud.

3.7.4.1. **SaaS: At CxOs level, Security Responsibilities and Objectives means.**

- 3.7.4.1.1. **Complete visibility to enterprise SaaS usage and risk profiling.**
- 3.7.4.1.2. **Governance of user access to SaaS and identity federation.**

3.7.4.2. **PaaS: At Application teams and different LOBs, Security Responsibilities and Objectives means.**

- 3.7.4.2.1. Enable developers to compose secure cloud applications and APIs, with enhanced user experience.
- 3.7.4.2.2. Visibility and protection against fraud and applications threats.

3.7.4.3. **IaaS: At CIO and IT teams levels, Security Responsibilities and Objectives means.**

- 3.7.4.3.1. Protect the cloud infrastructure to securely deploy workloads and meet compliance objectives.
- 3.7.4.3.2. Have full operational visibility across hybrid cloud deployments, and govern usage.

3.7.5. Cloud Security Capabilities.

3.7.5.1. **Identity: Manage identities and govern user access**

3.7.5.2. **Protection: Protect infrastructure, applications, and data from threats.**

3.7.5.3. **Insight: Auditable intelligence on cloud access, activity, cost and compliance.**

3.7.6. IaaS specific security considerations.

3.7.6.1. The definition of workload sensitivity will be determined by a Customer's:

- 3.7.6.1.1. Risk management framework.
- 3.7.6.1.2. Compliance obligations.

3.7.6.2. Typical examples of sensitive workloads include:

- 3.7.6.2.1. Sensitive personal information of employees, partners and clients.

- 3.7.6.2.2. Company confidential intellectual property, business plans and financial information.
 - 3.7.6.2.3. Data regulated by industry (e.g. PCI-DSS) or government (e.g. HIPAA-HITECH).
 - 3.7.6.3. When data or processing is moved to a cloud, the consumer retains the ultimate responsibility for compliance with data-related laws and regulations.
 - 3.7.6.4. Nonconformance with regulations can result in legal ramifications for both the customer and the provider depending on the regulation.
- 3.7.7. PaaS specific security considerations.
 - 3.7.7.1. Hardening and Securing the environment.
 - 3.7.7.2. Patch management for images.
 - 3.7.7.3. IDaaS: cloud-based services that broker identity and access management functions to target systems on customers' premises and/or in the cloud, IDaaS can be thought of as single sign-on (SSO) for the cloud.
- 3.7.8. SaaS specific security considerations
 - 3.7.8.1. **Business Challenge:**
 - 3.7.8.1.1. Extend on-premise IAM infrastructure to cloud apps.
 - 3.7.8.1.2. Secure employee access to SaaS applications (IBM, Google Apps, Salesforce).
 - 3.7.8.1.3. Manage identity and federated SSO for internal / traditional applications and new external SaaS ones.
 - 3.7.8.1.4. Provision / de-provision users in SaaS partner's registry.
 - 3.7.8.2. **Solution:**
 - 3.7.8.2.1. Common identity management solution for user provisioning and password management.
 - 3.7.8.2.2. Role-based provisioning and de-provisioning.
 - 3.7.8.2.3. User- and manager-initiated entitlement requests.
 - 3.7.8.2.4. BU administrators manage their users' rights.
 - 3.7.8.2.5. Federate access in context, based on web launch points; federated SSO access based on role.
 - 3.7.8.3. Current Security capabilities delivered as Cloud service.
 - 3.7.8.3.1. **Fraud Prevention.**
 - 3.7.8.3.2. **Mobile Security.**
 - 3.7.8.3.3. **Web Protection.**
- 3.7.9. BPaaS specific security considerations.
 - 3.7.9.1. Secure environment for securing and governing the implemented business processes definition, development, publish and subscription.

3.8. Describe high availability and DR as it pertains to cloud computing.

SUBTASK(S):

- 3.8.1. **Describe High Availability as it relates to “manage from” and “manage to” stacks in a cloud computing environment.**

- 3.8.1.1. **High Availability of “manage from” stack may be required to ensure the cloud continues to perform despite component failures**
- 3.8.1.2. **High Availability of “manage to” components ensures the workloads provisioned on the cloud are able to perform at the SLAs desired by the organization.**
- 3.8.2. **Describe the three types of storage required by cloud workloads.**
 - 3.8.2.1. **Transactional storage is required to support runtime computations in a cloud (such as database indexing, etc) which are considered “Tier 1” storage.**
 - 3.8.2.2. **Network attached storage is required to allow a customer to flexibly increase their file storage capacity.**
 - 3.8.2.3. **Fixed Content Storage contains objects that are written once and never modified but may be replaced (ie, records, image, video).**
- 3.8.3. **Define the areas of considerations for high availability of a cloud solution.**
 - 3.8.3.1. **Resilient virtual infrastructure ensures the underlying hardware that the workloads run on can withstand failures.**
 - 3.8.3.2. **Resilient Common Cloud Management Platform ensures the cloud computing management environment is highly available and builds on top of the resilient virtual infrastructure.**
 - 3.8.3.3. **Resilient Cloud Managed Services from the perspective of a Cloud Managed Service provider ensures the services delivered via the cloud are configured to be highly available.**
 - 3.8.3.4. **Resilient Cloud Managed Services being used together with partner applications in an end-to-end composite solution scope require all aspects of service composition to be highly available.**
- 3.8.4. **Define RTO and RPO:**
 - 3.8.4.1. **Recovery Time Objective (RTO)** specifies the duration of time within which a business process must be restored after a disaster.
 - 3.8.4.2. **Recovery Point Objective (RPO)** specifies the point in time to which data must be recovered, measured backwards from the time of occurrence of the disaster.
- 3.8.5. **Define DR topologies and configurations as it relates to cloud computing**
 - 3.8.5.1. **Describe DR topologies that can be leverage to provide optimal RTO/RPO. These topologies can be defined as Single Primary / Single Secondary, Multiple Unrelated Primary / Single Secondary, Hybrid Cloud: Multiple Related Primaries and the configurations as Frozen DR, Cold DR, Warm DR, Hot DR and Active/Active DR.**

3.9. Define four defining principles of Cloud computing as presented in the IBM CCRA V4.

SUBTASK(S):

- 3.9.1. **Efficiency Principle - Design for cloud-scale efficiencies:**
When realizing cloud characteristics such as elasticity, self-service access, and flexible sourcing, the cloud design is strictly oriented to high cloud scale efficiencies and short time-to-delivery/time-to-change.

To implement a cloud following this principle with that high level of efficiency and flexibility, a very high degree of standardization (i.e. minimal variety in the data center with respect to numbers of server, storage, network technologies, operating systems & versions, middleware products, applications, etc.) is required to enable high degrees of automation. The higher the degree of standardization / minimization of variety are, the better automation can be realized (assuming a well-integrated and interoperable set of management components). In a highly homogeneous public cloud data center this can be achieved more effectively compared to private cloud enterprise data centers running a variety of workloads each of them having different requirements, so there is typically a trade-off between degree of standardization and level of efficiency.

3.9.2. Lightweightness Principle – Support lean service management:

The CCMP fosters lean and lightweight service management policies, processes, and technologies.

Fundamental restructuring and streamlining of IT management processes is required to maximize the elimination of manual data center management tasks. The main factors for reducing operational costs are elimination of tasks which are not needed any more due to limited scope of managed (e.g. in compute cloud only managing up to and including the hypervisor) and optimization (e.g. not immediate repair of a failed physical machine enabled by automated restart of crashed VMs or nodes or automating the service activation process, which is typically very time- and cost-intensive in traditional outsourcing environments).

3.9.3. Economies-of-scale Principle – Identify and leverage Commonalities:

All commonalities are identified and leveraged in cloud service design. In this principle the goal is to reuse management/CCMP components and enable Economies-of-scale (with respect to initial standup & operational costs and reduced time-to-market) by sharing a single/common management platform to deliver and manage many cloud services. Examples of components with reuse potential are metering, monitoring, service automation, management User Interface (UI) components etc.

3.9.4. Generic Principle – Define and manage generically along the lifecycle of cloud services:

Be generic across IaaS, PaaS, SaaS, BPaaS and provide ‘exploitation’ mechanism to support various cloud services by using a shared management platform. It is essential to introduce a model which allows cloud service developers to specify how the CCMP functionality gets used in the context of their specific cloud service and how – based on that definition or template – instances of that cloud service get delivered to cloud service consumers. This has been taken into account in the CCMP RA design. The remaining task for the cloud management platform architect is to design how the CCMP management functionality gets exploited in the context of the respective cloud service. This is achieved by creating a set of service type-specific artifacts as required by the respective management platform components (e.g. cloud service-specific scripts, monitoring agents, etc.).

3.10. Describe Cloud Service Consumers, Cloud Service Creators, Cloud Service Provider, Cloud Services and the Common Cloud Management Platform.

SUBTASK(S):

- 3.10.1. Explain the role of the Cloud service consumer:
Cloud service consumers require a simplified interface with well-defined service offerings, pricing and contracts.
 - 3.10.1.1. The cloud service consumer is the individual, organization or system which consumes service instances delivered by a particular cloud service.
 - 3.10.1.1.1. Examples of service consumption are requests for virtual servers, changes to CPU capacity, requests for storage based on pre-defined templates, etc...
 - 3.10.1.2. Cloud service consumers browse the service offering catalog and trigger service instantiation requests.
- 3.10.2. Explain the role of the Cloud service provider:
Cloud service providers are the owners of the CCMP, and are responsible for providing cloud services to the cloud service consumer.
 - 3.10.2.1. The cloud service provider may itself be a consumer of the CCMP (in a hosted SaaS offering for example), or they may be running the CCMP themselves.
- 3.10.3. Explain the role of the Cloud service creator:
Cloud service creators are responsible for creating the services being offering in the cloud services offering.
 - 3.10.3.1. Cloud service creators produce their cloud services by leveraging and enhancing functionality exposed by the cloud service provider.
 - 3.10.3.2. Cloud service creators would be responsible for the design, testing, implementation and maintenance of management artifacts specific to a cloud service.
 - 3.10.3.3. The cloud service creator can be an organization (e.g., ISV company) or an individual (e.g., business/technical specialists in the ISV creating services)
- 3.10.4. Describe Cloud Services as defined by the IBM CCRA V4:
 - 3.10.4.1. There are 4 categories of cloud services: IaaS, PaaS, SaaS, BPaaS
 - 3.10.4.2. In contrast to traditional IT services, cloud services have attributes such as pay-per-usage, self-service usage, flexible scaling and shared-usage.
- 3.10.5. Describe the CCMP:
 - 3.10.5.1. The CCMP architecture is responsible for delivering instances of cloud services of any category to cloud service consumers, in an ongoing, self-service fashion.
 - 3.10.5.2. The infrastructure element layer relates to the hardware infrastructure such as facilities, servers, storage, and network resources.

- 3.10.5.2.1. No software or hypervisor, or virtualization management software is included in this infrastructure layer.
- 3.10.5.2.2. The infrastructure is managed by the OSS part of the CCMP.
- 3.10.5.3. The CCMP exposes a set of BSS and OSS:
 - 3.10.5.3.1. BSS Examples – Customer account management, service offering catalog/management, contracts/agreement management, service request management, order management, pricing, entitlement management, subscription management, metering, rating, billing, accounts payable, accounts receivable, clearing and settlement.
 - 3.10.5.3.2. OSS Examples – Service delivery catalog, service automation management, service request management, change & configuration management, image lifecycle management, provisioning, incident & problem management, IT service level management, monitoring & event management, IT asset & license management, capacity & performance management and platform & virtualization management.

3.11. Describe how IBM Service Management can effectively manage a customer's cloud environment.

SUBTASK(S):

- 3.11.1. Describe the concepts of Service Oriented Architecture (SOA) at a high level. SOA is a set of components which can be invoked, and whose interface descriptions can be published and discovered. It defines how to integrate disparate applications for a web-based environment while using various implementation platforms.
- 3.11.2. Describe how cloud computing supports efforts to establish a service-oriented architecture and to enhance service management. SOA is the process of defining and IT solution or architecture, while cloud computing is an architectural alternative. The software services are supported by the SOA platform, which typically include components such as ESB and a service registry. The SOA platform is supported by the enterprise IT infrastructure of systems, data and networks. These elements of SOA also relate to different kinds of cloud services. The software services relate to SaaS, the infrastructure to IaaS.
- 3.11.3. Describe the components of service management for cloud computing.
 - 3.11.3.1. Service Delivery and Process Automation.
 - 3.11.3.2. Service Availability and Performance Management.
 - 3.11.3.3. Storage Management.
 - 3.11.3.4. Security, Risk and Compliance.
 - 3.11.3.5. Data center Transformation.
 - 3.11.3.6. Asset and Financial Management.

- 3.11.3.7. Network and Service Assurance.
- 3.11.4. Describe the components and benefits of Service Management in terms of visibility, control and automation.
 - 3.11.4.1. Visibility – all elements and services (including assets, server, storage network, virtual and logical elements and relationships for configuration, availability, security and performance).
 - 3.11.4.2. Control – policies to assure service delivery and compliance, including the correlation of resources with desired compliance patterns.
 - 3.11.4.3. Automation – data center processes from element run-books to broad provisioning and compliance scenarios.

3.12. Describe the Integration and Extensibility models of cloud solutions described in CCRA V4.

SUBTASK(S):

- 3.12.1. Integration points for CEDC cloud adoption pattern – Describe how to integrate the IBM components that implement a CEDC component. Describe also how to integrate the IBM core cloud components, with third-party products in the areas of Endpoint Security, Monitoring, Backup & restore, Event Management and ITIL process management.
- 3.12.2. Integration points for Platform Services cloud adoption pattern – Describe the major integration scenarios in a PaaS environment including:
 - 3.12.2.1. Application integration points defined by the PaaS solution
 - 3.12.2.2. Application integration points used by PaaS solution for cloudbursting scenarios.
 - 3.12.2.3. Data migration.
 - 3.12.2.4. Data Synchronization.
 - 3.12.2.5. Data Exposition.
 - 3.12.2.6. Monitoring and management of cloud integration points.
- 3.12.3. Identify and describe the major components that implement cloud integration and extension services for PaaS environments (Cast Iron, Worklight, IBM Endpoint Manager).
- 3.12.4. Integration points for Cloud Service Providers cloud adoption pattern – Describe the major integration scenarios in Cloud Service Provider environments including:
 - 3.12.4.1. Integration across IBM components realized through SmartCloud Aggregator /Cast Iron solution.
 - 3.12.4.2. Integration with external rating, charging and billing frameworks.
 - 3.12.4.3. Integration with existing Firewalls, Balancers and AAA solutions.
 - 3.12.4.4. Integration with Storefronts from our business partners (i.e. Parallels and JamCracker).
- 3.12.5. Integration points for Building SaaS cloud adoption pattern - Describe the major integration scenarios in SaaS environments including:
 - 3.12.5.1. Integration with recommended tools like proxy servers, IP and network traffic management, data and analytic platforms, load balancers and network appliances.

- 3.12.5.2. Use of Cast Iron and integration solutions for exposing services or for using services from other SaaS environments.

3.13. Understand the role of governance in the CCRA.

SUBTASK(S):

- 3.13.1. Define the governance model for a cloud deployment.
 - 3.13.1.1. Utilize existing policies, or define new policies, of the Cloud Service Provider that have relevance to the Cloud environment.
 - 3.13.1.2. For human governance policies, define the policies in employee practices to be followed.
 - 3.13.1.3. For business/machine governance policies, define the policies in rules to be monitored and/or audited.
- 3.13.2. Deploy the policies.
 - 3.13.2.1. For human policies, produce or extend the employee handbook (or equivalent).
 - 3.13.2.2. For business policies, include the policies in business processes (manual and automated).
 - 3.13.2.3. For machine policies, define rules to be deployed to policy definition and policy enforcement systems.
 - 3.13.2.4. For auditing policies, define rules to be deployed to auditing systems.

3.14. Describe non-functional requirements (NFRs) in the context of a cloud solution.

SUBTASK(S):

NFRs identify critical aspects of the cloud solution that are not feature/function related. NFRs impact the solution design by clearly identifying key characteristics of cloud operations.

- 3.14.1. Availability and serviceability includes characteristics such as high availability, DR, acceptable downtime or degradation of services during maintenance. The availability expectations of a system relate to how many hours in the day, days per week, and weeks per year the application is going to be available to its users and how quickly they should be able to recover from failures. Since the system includes Software (including applications), Hardware and Network components, this requirement extends to all three types. The serviceability expectations must integrate with existing support structure and support processes, provide a ticketing system to log/track problem tickets and that integrated with an existing ticketing system, support automatic patch download and installation and provide sufficient diagnostic information (logs, dumps, traces) to expedite problem resolution and support service level agreements often measured by key performance indicators (KPIs) like “98.5% availability” or “Full restoral to service in < 4 hrs” or “Maintenance window limited to a two hour window once per month on second Saturday”.
- 3.14.2. Performance includes UI and VM expected performance. The cloud infrastructure and services must be able to meet the response time, throughput

and scaling requirements as defined by the service level agreements of the service offering. The cloud infrastructure must provide manual and automated ways to optimize utilization in the data center. Often measured by KPIs like “64 bit RHEL VM should be available within eight minutes of user provisioning request” or “UI responsiveness should render catalog options within 5 seconds”.

- 3.14.3. Scalability includes number of concurrent users and number of number of managed workloads and number of VMs per minute/hour. Scalability is the ability to expand the system architecture to accommodate more users, more transactions and more data as users and data are added. This should allow existing systems to be extended as far as possible without necessarily having to replace them. Often measured in KPIs like “Needs to support 100 concurrent users” or “Should have capacity to managed 10,000 RHEL VMs and 5,000 AIX LPARs” or “System should be able to provision 100 RHEL VMs per/hour”.
- 3.14.4. Consumability includes UI usability, cloud infrastructure install time and total cost of ownership. Consumability is a description of the customer’s end-to-end experience with the solution. The tasks associated with Consumability start before the consumer purchases a service and continue until the customer stops using the product. By improving the Consumability of the service, the value of that service to the client can be increased. Often quantified as “UI should be intuitive for new users without formal training” or “Installation of cloud infrastructure should require no more than 80 hours”.
- 3.14.5. Extensibility includes 3rd party integration, UI extensibility, application interfaces, and hypervisor support. The Cloud must be extensible in order to address future functionality and changes without having to be rewritten, support that the application may have access to additional disparate back-end systems, support the ability to integrate with existing security systems either on-premise or elsewhere in clouds and be able to add/remove/relocate physical and logical resources without disturbing running services. Often quantified as “Cloud infrastructure should interface with existing problem management system” or “Cloud infrastructure should support Vmware, PowerVM, and HyperV” or “Self Service UI should be invocable through RESTful APIs”.
- 3.14.6. Security includes Command & Control, Identity, Access, and Entitlement Management, Data and Information Protection Management, Software, System, and Service Assurance, Threat and Vulnerability Management, Risk and Compliance Assessment and Security Policy Management. Often driven by industry regulatory compliance. Often quantified as “Must adhere to corporate standard XYZ” or “Provisioned VMs must receive monthly security updates” or “Cloud infrastructure should ensure network isolation between tenant workloads”.

3.15. Describe the objectives of the Mobile Pattern in the CCRA.

SUBTASK(S):

The objective of the mobile pattern in the CCRA is to learn the cloud deployment options of the solution components that:

- 3.15.1. build mobile apps for bringing business functionalities in existing business applications, new enterprise functionality built for mobile, business solutions, business processes and business performance on mobile devices
- 3.15.2. Protect the BYOD devices and the mobile end points and prevents fraud and secure the mobile ecosystem
- 3.15.3. Engage with mobile app and Web users at the optimal time and place, and analyze customer behavior and customer experience

For more information review IBM MobileFirst & Cloud Computing

Section 4 - IBM Cloud Computing Solutions

4.1. Demonstrate understanding of IBM's cloud offerings for Infrastructure as a Service solutions.

SUBTASK(S):

- 4.1.1. Describe which cloud offering can be used for a on-premise cloud IaaS solution
 - 4.1.1.1. IBM SoftLayer - Provides flexibility and choice in managing workloads with options to use bare metal or virtualized, dedicated or shared servers. Offers best-in-class performance and latency with our dark-fiber overlay network.
- 4.1.2. Describe which cloud offering provides a fully managed infrastructure
 - 4.1.2.1. IBM Cloud Managed Services - A fully managed, security-rich and production-ready cloud environment designed to ensure enterprise-class performance and availability. It offers complete governance, administration and management control along with service-level agreements (SLAs) to align your specific business and usage requirements. Multiple security and isolation options built into the virtual infrastructure and network keep this cloud separate from other cloud environments.
- 4.1.3. Describe which cloud offering enables the management of public, private and hybrid clouds
 - 4.1.3.1. IBM Cloud Orchestrator - A unified cloud management platform which fully automates the deployment and lifecycle management of cloud services across compute, network and storage resources. Includes pattern deployment engine as well as a flexible data center orchestration tool.

4.2. Describe the management support differences of Platform as a Service offerings between- on and off premise use.

SUBTASK(S):

- 4.2.1. Support delivery for a full-service Platform as a Service is different than support for commercial packaged software or a subscription service for several reasons:
 - 4.2.1.1. PaaS offering patches/ fixes on an ongoing basis with no service interruption, using continuous deployment. The Platform is designed to support the continuous deployment process.
 - 4.2.1.2. The core services of the PaaS offerings are in constant use by thousands of users. Monitoring capabilities mean the provider knows about an issue before consumer.
- 4.2.2. Benefits of PaaS service offerings are:
 - 4.2.2.1. Support for applications written using a variety of languages and frameworks.
 - 4.2.2.2. Scale-out architecture of PaaS is fully replicated by design, so if a server fries, you just lose a little performance until you snap in a new one.
 - 4.2.2.3. PaaS enables enforcement the same application development policies and procedures across languages and frameworks.

- 4.2.3. Explain difference between supporting on prem vs. off prem PaaS development
 - 4.2.3.1. Off-premise PaaS solution means no worries about anything infrastructure for anyone within the organization. On the other hand, an off-premise premise PaaS solution comes with the same baggage as off-premise IaaS offerings: a lack of control and visibility into the infrastructure. Visibility and control that is often considered critical to maintaining performance of applications and applying appropriate security and access control policies.
 - 4.2.3.2. On-premise PaaS comes with a larger price tag and a longer time to implement, both of which may be show-stoppers for those organizations that cannot risk capital or time. Forward looking capable organizations, on-premise PaaS will ultimately offer both the reduction in costs (over time) as well as the highly desirable operational benefits without compromising on visibility or control.
- 4.2.4. List the solutions and products that implement the adoption pattern.
 - 4.2.4.1. The Platform Services adoption pattern describes methods to provide application development and deployment environments, middleware deployment and management environments, and cloud integration services where the consumer has access to the data and applications for the platform, but not the underlying supporting infrastructure.
 - 4.2.4.2. Solutions prescribed to implement the patterns:
 - 4.2.4.2.1. IBM SmartCloud Continuous Delivery
 - 4.2.4.2.2. IBM Bluemix
 - 4.2.4.2.3. IBM Workload Deployer
 - 4.2.4.2.4. IBM PureApplication Systems
 - 4.2.4.2.5. IBM PureApplication Service on SoftLayer
 - 4.2.4.2.6. Rational Asset Manager
 - 4.2.4.2.7. Rational Automation Framework
 - 4.2.4.2.8. IBM Cloud Managed Services for SAP Applications
 - 4.2.4.2.9. IBM Cloud Managed Services for Oracle Applications

4.3. Describe how IBM Cloud Computing products and solutions can be leveraged to design and provide an effective Software as a Service (SaaS) solution.

SUBTASK(S):

- 4.3.1. **Implement Existing Applications to be Delivered as SaaS solutions** – Includes analysis of a non-cloud application to understand the application's platform requirements (operating system, middleware, code libraries, etc.) and cloud characteristics (multi-tenancy, service oriented architecture, etc.); implementation of application modifications to enable cloud services; and definition of the required cloud infrastructure and platform environment for the application. Describes the major logical components that allow to build a SaaS solution and how the below components map to the corresponding IBM products that realize them.
 - 4.3.1.1. **Cloud Platform Technology.**

- 4.3.1.1.1. IBM SmartCloud Orchestrator.
 - 4.3.1.1.2. Application Patterns.
 - 4.3.1.1.3. IBM Security AppScan.
 - 4.3.1.1.4. IBM Security Network Intrusion Protection System Virtual Appliance (GV).
- 4.3.1.2. **Cloud Implementation.**
 - 4.3.1.2.1. Application Development as a Service.
- 4.3.1.3. **Cloud Migration Services.**
 - 4.3.1.3.1. Cloud Application Modernization.
 - 4.3.1.3.2. Migration Services for Cloud.
- 4.3.1.4. **Expert Integrated Systems.**
 - 4.3.1.4.1. IBM PureApplication System.
 - 4.3.1.4.2. Application Patterns.
 - 4.3.1.4.3. IBM PureApplication System on Power.
 - 4.3.1.4.4. IBM PureData Systems 3 favors.
- 4.3.1.5. **Platform as a Service.**
 - 4.3.1.5.1. IBM SmartCloud Application Services.
 - 4.3.1.5.2. IBM PureApplication Service on SoftLayer Beta.
- 4.3.1.6. **Infrastructure as a Service.**
 - 4.3.1.6.1. SoftLayer.
 - 4.3.1.6.2. IBM Cloud Managed Services.
 - 4.3.1.6.3. IBM Platform Computing Cloud Service.
 - 4.3.1.6.4. IBM Managed Infrastructure for Private Cloud.
- 4.3.2. **Implement Cloud Native Applications to be Delivered as SaaS solutions -**
 Supports the development of applications which leverage cloud-based capabilities such as massive scalability, loosely coupled application services (service-orientation) and application-layer built-in high-availability/redundancy, delivered via automatic, elastic scaling of resources. The applications may include integrated tools and use services provided by other cloud business processes and applications. Describes the major logical components that allow to build a SaaS solution and how the below components map to the corresponding IBM products that realize them.
 - 4.3.2.1. **Cloud Platform Technologies.**
 - 4.3.2.1.1. IBM SmartCloud Orchestrator.
 - 4.3.2.1.2. Application Patterns.
 - 4.3.2.1.3. IBM Security AppScan.
 - 4.3.2.1.4. IBM Security Network Intrusion Protection System Virtual Appliance (GV).
 - 4.3.2.2. **Cloud Implementation.**
 - 4.3.2.2.1. Application Development as a Service.
 - 4.3.2.3. **Expert Integrated Systems.**
 - 4.3.2.3.1. IBM PureApplication System.
 - 4.3.2.3.2. Application Patterns.
 - 4.3.2.3.3. IBM PureApplication System on Power.
 - 4.3.2.4. **Platform as a Service.**
 - 4.3.2.4.1. IBM Bluemix.

- 4.3.2.4.2. IBM SmartCloud Application Services.
 - 4.3.2.4.3. IBM PureApplication Service on SoftLayer.
 - 4.3.2.4.4. IBM Mobile Innovation in the Cloud.
 - 4.3.2.4.5. Cloud Mobile Managed Services.
 - 4.3.2.5. **Infrastructure as a Service.**
 - 4.3.2.5.1. SoftLayer .
 - 4.3.3. **Consume SaaS Applications -** Allows for the use of applications and business processes which are delivered from a cloud service in accordance with an SLA. Architectural considerations include scalability, standardization, user management and provisioning, data exchange with the SaaS provider, security and manageability. Describes the major logical components that allow to build a SaaS solution and how the below components map to the corresponding IBM products that realize them.
 - 4.3.3.1. **IBM Cloud Marketplace** – an excellent starting place to learn about IBM SaaS offering by solution areas. While it provides a large number of IBM SaaS solutions, it does not provide an exhaustive list.
 - 4.3.4. **Integrate SaaS with Cloud and Enterprise Services -** Provides the ability to integrate with existing enterprise applications and business processes as well as with services management software and, potentially, with usage and accounting systems. Describes the major logical components that allow to build a SaaS solution and how the below components map to the corresponding IBM products that realize them.
 - 4.3.4.1. **Platform as a Service.**
 - 4.3.4.1.1. IBM WebSphere Cast Iron Live.
 - 4.3.4.1.2. IBM WebSphere Cast Iron Express.
 - 4.3.4.1.3. IBM BlueMix.
 - 4.3.4.2. **Hybrid Cloud Technologies.**
 - 4.3.4.2.1. IBM API Management.
 - 4.3.4.2.2. IBM WebSphere Cast Iron.
- 4.4. Explain the concept of a Define Database As A Service (DbaaS) and how it relates to a SaaS, IaaS and PaaS or any CCRA adoption pattern in a cloud computing environment.**

SUBTASK(S):

The concept of a database as a service model is:

- 4.4.1. A Database-as-a-Service (DBaaS) is a service that is managed by a cloud operator (public or private) that supports applications, without the application team assuming responsibility for traditional database administration functions. There are two common deployment models: users can run databases on the cloud independently, using a virtual machine image, or they can purchase access to a database service, maintained by a cloud database provider. Of the databases available on the cloud, some are SQL-based and some use a NoSQL data model.

DbaaS use cases: A DbaaS can be used to offset costs of keeping millions of rows of data locally, data archivals, data backup, and data recovery. Here are some examples as it relates to cloud adoption patterns

- 4.4.1.1. PaaS: A DbaaS can serve as a database layer built on open source databases, noSQL database solutions, data warehouse, master data management (MDM), and/or enterprise solutions such as DB2 and MySQL as part of an overall PaaS cloud platform environment in support of a common computing platform. For example, a database layer is required for web application development or a reporting and analytics PaaS environment. To meet the growing needs of those PaaS environments, a DbaaS can be used to extend the data layer. IBM's Cloudant acquisition can provide these capabilities as well as offerings provided by BlueMix, SoftLayer and IBM's Cloudera business partner.
- 4.4.1.2. IaaS: DbaaS can serve as a database layer built on open source databases, noSQL data providers or enterprise solutions such as DB2 and MySQL. The platform selection would be the core infrastructure and in cloud service provider environment can serve as the IaaS. The appropriated database software would then be installed and any management clients and tools can also be installed on the infrastructure or appropriate computing environment to access that database. IBM SoftLayer can offer bare metal to create the infrastructure for a DbaaS as well as an IaaS built on Power, x86 and more to create a DbaaS cloud computing environment.
- 4.4.1.3. A DbaaS, with database related software that provides a computing solutions is part of an overall SaaS solution. An example would be MaaS 360 and SmartCloud Control Desk, and Emptoris contract management software where the a database component can grow and a DbaaS may be needed to manage data growth.
- 4.4.2. An on-prem DbaaS cloud computing environment is a a DbaaS environment that is part of the client's on-site computing environment.
- 4.4.3. Examples of how a DbaaS environment can solve a client's data layer needs in an overall computing environment are: Archival solutions, Big Data solutions, reporting and advanced analytics, and an extended database environment in support of a business application to offset the workload.

4.5. Define considerations of storage and data recovery in an IBM Cloud Solution also taking into consideration the different types of storage and how to use them in the different cloud environments.

SUBTASK(S):

- 4.5.1. Explain considerations of storage and data recovery in an IBM Cloud Solution
 - 4.5.1.1. Cloud general storage requirements:
 - 4.5.1.1.1. Scalability; low cost.
 - 4.5.1.1.2. Dynamic, unpredictable workloads.
 - 4.5.1.1.3. Automated management, provisioning, performance monitoring and tuning.

- 4.5.1.1.4. Security and data protection.
- 4.5.1.1.5. Quality of Storage Service.
- 4.5.1.1.6. Geographic distribution.
- 4.5.1.1.7. Storage use cases:
 - 4.5.1.1.7.1. Backup
 - 4.5.1.1.7.2. Archive
 - 4.5.1.1.7.3. Database
 - 4.5.1.1.7.4. File
 - 4.5.1.1.7.5. Block
- 4.5.1.2. Compute Clouds: Private and public Compute Clouds include storage within the compute service.
 - 4.5.1.2.1. Storage capacity and data protection are directly delivered in this model.
 - 4.5.1.2.2. Storage Infrastructure to achieve the most efficient implementation.
 - 4.5.1.2.3. Use case example; SaaS, IaaS.
- 4.5.1.3. Storage Clouds.
 - 4.5.1.3.1. Storage Capacity Clouds – obtain storage for data from a cloud service.
 - 4.5.1.3.2. Backup Clouds – protect data, applications and business services to a backup cloud service.
 - 4.5.1.3.3. Archive and Disaster Recovery Clouds – archive data or create offsite data copies via a cloud service.
 - 4.5.1.3.4. Records Management Clouds – data aware archive services, often aligned with specific market formats
- 4.5.2. Content Clouds – services that deliver or receive content streams such as video on demand, medical imaging, surveillance data, etc.
- 4.5.3. Determine the storage design characteristics appropriate for a deployment.
 - 4.5.3.1. Determine the application requirements for data persistence, for both transient storage needs and persistent storage needs.
 - 4.5.3.2. For persistent storage needs, determine the need for exclusive or shared access.
 - 4.5.3.3. For persistent storage needs, determine the need for storage locality with the VM.
 - 4.5.3.4. For persistent storage needs, determine the capacity, volume to transmit and latency requirements across applications using the storage.
- 4.5.4. Determine the storage technologies suitable for the architecture defined either elastic or non elastic, etc.
 - 4.5.4.1. Is local storage sufficient to meet storage capacity needs.
 - 4.5.4.2. Is a storage controller required to meet capacity, sharing and throughput needs.
- 4.5.5. Determine additional external functions required related to the data being stored.
 - 4.5.5.1. If backup/restore functions are being provided, determine if the storage function supports locking requirements to support backup/restore.
 - 4.5.5.2. If snapshot functions are being provided, determine if the storage function supports locking requirements to support snapshot.

4.6. Define service orchestration as it pertains to Cloud Computing.

SUBTASK(S):

- 4.6.1. Define service orchestration as it pertains to cloud computing.
 - 4.6.1.1. Cloud service orchestration is composing of architecture, tools and process within a defined service, such that the provisioning of the defined service is provided by stitching of software and hardware components together via automated workflows.
 - 4.6.1.2. Cloud service orchestration is critical in the delivery of cloud computing because it fulfills assurance and billing, and enables the delivery of complex services in technical and business domains.
- 4.6.2. Define the three services tiers that orchestration in cloud computing spans.
 - 4.6.2.1. The Infrastructure tier pertains to the underlying virtual machines, availability zones, scaling rules and security groups that are utilized to provision a service.
 - 4.6.2.2. The Service tier is comprised of operating systems, middleware and configuration items that make up the service being delivered
 - 4.6.2.3. The Application tier is comprised of the code & configuration that makes up the application as part of the service delivery.
- 4.6.3. Define the role of orchestration in cloud computing. Orchestration plays a role in the entire life cycle of a service in cloud computing, spanning:
 - 4.6.3.1. Initialization pertains to the initial provisioning to deliver a set of h/w and s/w components stitched together via a workflow to provision a complex service.
 - 4.6.3.2. Steady State support is provided by orchestration by identifying the components and mechanisms for monitoring all aspects of the service
 - 4.6.3.3. Change Management support ensures any changes to the service (such as responding to scaling events, security patching, etc) are handled securely and accurately.
- 4.6.4. Demonstrate understanding of IBM's service orchestration solutions:
 - 4.6.4.1. IBM SmartCloud Orchestrator: A unified cloud management platform which fully automates the deployment and lifecycle management of cloud services across compute, network and storage resources. Includes pattern deployment engine as well as a flexible data center orchestration tool.
 - 4.6.4.2. IBM UrbanCode Deploy: IBM UrbanCode Deploy orchestrates and automates the deployment of applications, middleware configurations and database changes into development, test and production environments. This software enables your team to deploy as often as needed – on demand or on a schedule, and with self-service. UrbanCode Deploy can help your team to accelerate their time to market, drive down costs and reduce risk.
 - 4.6.4.3. IBM PureApplication Services on SoftLayer: IBM SmartCloud Application Services runs on, and automatically deploys virtual resources on

SoftLayer (IaaS). SmartCloud Application Services leverages IBM's pattern deployment engine.

Next Steps

1. Take the [CCRA V4](#) assessment test using the promotion code *ccstudy* for \$10 (\$20 USD savings).
2. If you pass the assessment exam, visit pearsonvue.com/ibm to schedule your testing sessions. Use the promotion code *ccguide* to receive 20% off.
3. If you failed the assessment exam, review how you did by section. Focus attention on the sections where you need improvement. Keep in mind that you can take the assessment exam as many times as you would like (\$10 per exam), however, you will still receive the same questions only in a different order.