Organizational Readiness and change Management in the cloud Age

Introduction

- The studies for Organization for Economic Co-operation and Development (OECD) economics demonstrated that there is a strong correlation between changes in organization and workplace practices and investment in IT.
- In order to effectively enable and support enterprise business goals and strategies, IT must adapt new technologies and continually change.
- Organization should have a transition to a desirable level of CMM (Change Management Maturity) by having following key knowledge:
  - Domain 1: Managing the Environment, understanding the organization (people, process and culture)
  - Domain 2: Recognizing and Analyzing the Trends (Business and Technology), observer the key driver for changes.
  - Domain 3:Leading for Results, Assess organizational readiness and architect solution that delivers definite business values.

Basic Concept of organizational readiness

- People in the organization face the change as challenging. They have fear or uncertainties. This is called FUD syndrome: Fear, Uncertainty and Doubt.
- Employees are used to their roles and responsibility and are familiar with their environment and management's expectations.
- But when corporate changes are made, it is common that people tend to become uncomfortable and excited regardless the level and intensity of change.
- Surveys are made and studies say that project fails to meet the objectives, money are wasted, opportunities are lost due to lack of focus and interest in the change.

Drivers for changes: A framework to comprehend the competitive environment

- The five driving factors for change given by the framework are:
  - 1) *Economic (global and local, external and internal)*

    Economic factors are usually dealing with the state of economy, both local and global in scale. Managers and groups are expected to deal with the unpleasant facts of shrinking market share, declining profit margins, unsatisfactory earnings, new and increasing competition. Managers are often asked to do more with less, and this is done during downturn.
  - 2) *Legal, political, and regulatory compliance*

    This deals with issues of transparency, compliance and conformity. The objective is to be a good corporate citizen and industry leader and to avoid the potential cost of legal threats from external factors.

- *Environmental (industry structure and trends)*

  Environmental factors usually deal with the quality of natural environments, human health, and safety.
- *Technology developments and innovation*

  New technologies and innovations in every has played very important part and has changed the lives of so many fields.
- *Socio cultural (markets and customers)*

  It sees the societal expectations and trends and how cloud computing change the world of markets and customers.

Creating a winning environment

- At the cultural level of an organization, change too often requires a lot of planning and resource. The management and executives communicate employees to make sure that every employee understands
  - 1) The new direction of the firm
  - 2) The urgency of the change needed
  - 3) What the risks are to – maintain status quote and making the change.
  - 4) What the new role of the employee will be
  - 5) What the potential rewards are.

  Build the business savvy organization

Common change management models

- There are many different change management approaches and models.
- **1) Lewin's Change Management Model**

  Kurt Lewin, a psychologist by training, observed that there are three stages of changes, which are ***Unfreeze, Transition and Refreeze.***

  It is recognized that people tend to become comfortable in this freeze or unchanging environment and they wish to remain in this safe/comfort zone. Any disturbance to them will make them uncomfortable.

  To encourage change, its necessary to unfreeze the environment by motivating people to accept the change. Motivation for change must be generated before change can occur. This is the unfreezing stage from which change begins.

  The transition phase is when the change plan is executed and actual change is being implemented.

  The last phase is Refreeze, this is the stage when the organization once becomes unchanging/fozen until the next time a change is initiated.

2) Deming Cycle(Plan, Do, Study, Act)

- The Deming cycle is also known as the PDCA cycle.
- It is a continuous improvement model with four sequential sub processes: Plan, Do, Check and Act.
- The PDCA cycle is usually implemented as an evergreen process, which means that the end of one complete cycle or pass flows into the beginning of the next pass and thus supports the concept of continuous quality improvement.
- **PLAN** : Recognize an opportunity and plan a change.
- **DO** : Execute the plan in a small scale to prove the concept.
- **CHECK** :Evaluate the performance of the change and report the results to sponsor.
- **ACT** : Decide on accepting the change and standardizing it as a part of the process.

Incorporate what has been learned from the previous steps to plan new improvements and begin a new cycle.

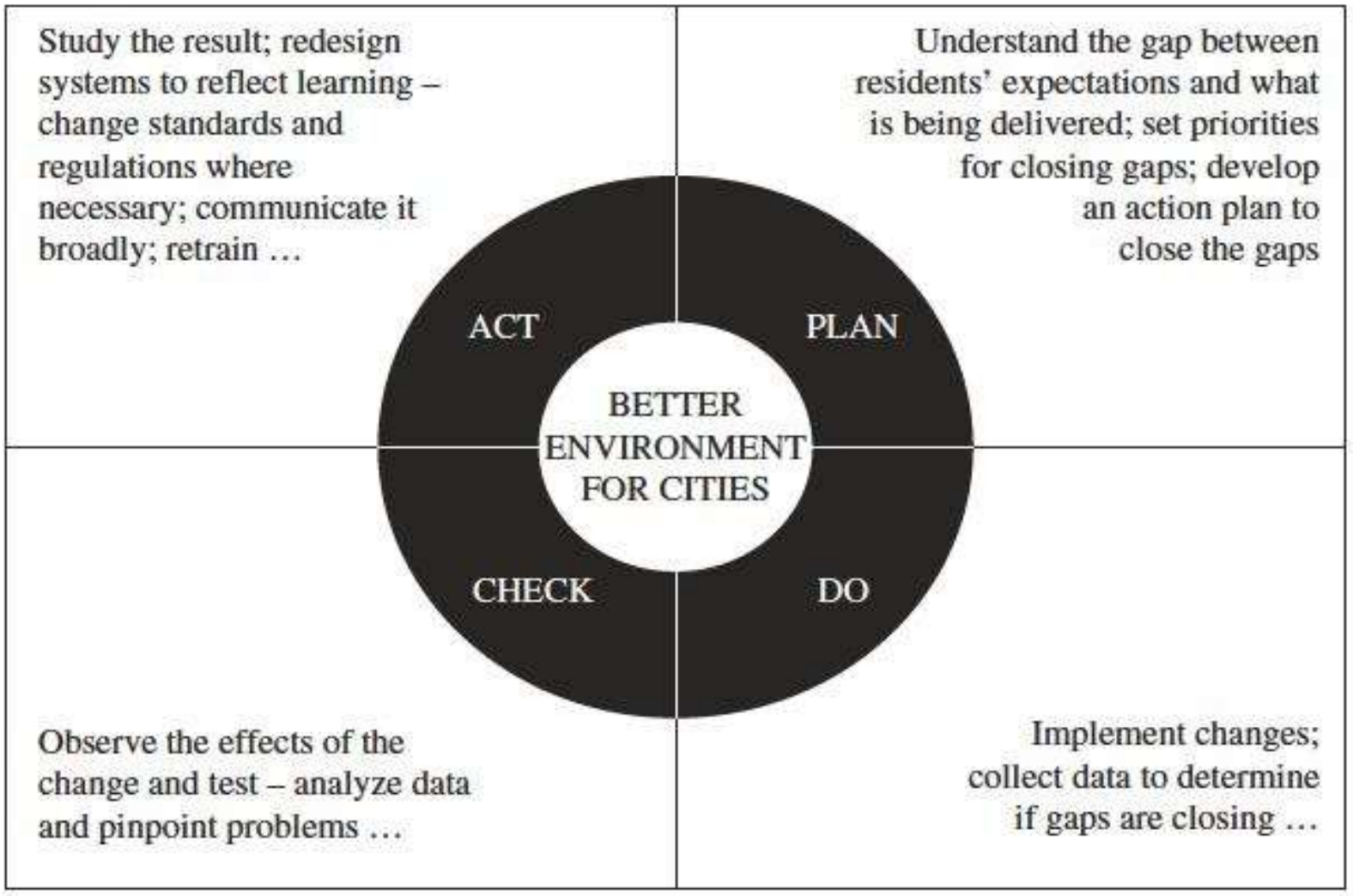


FIGURE 22.1. Deming's PDCA cycle.
Source: http://www.gdrc.org/uem/iso14001/pdca cycle.gif.

A Proposed Working Model : CROPS

- CROPS framework is a working model which stands for Culture, Rewards, Organization and Structures, Process, Skills and Competencies
- ***Culture :*** Corporate culture is a reflection of organizational (management and employees) values and belief.

  The culture of a group can be defined as, A pattern of shared basic assumptions that the group learned as it solved its problems of external adaption and internal integration, that has worked well enough to be considered valid and therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems.

Elements of organizational culture includes:

- Stated values and belief
- Expectations for member behavior
- Customs and rituals
- Stories and myths about the history of the organization
- Norms, the feelings evoked by the way members interact with each other
- Metaphors and symbols

- ***Rewards and Management System*** : This management system focuses on how employees are trained to ensure that they have the right skills and tools to do the right job. It identifies how to measure employee job performance and how company compensates them based on their performance. Reward is the most important that shapes employees values and beliefs.
- ***Organization and Structures*** : How the organization is structured is largely influenced by what the jobs are and how the jobs are performed. Business processes need to align with organizational vision, mission, and strategies in order to create customer and shareholder values.
- ***Process*** : Business process or business method as a collection of related, structured activities or tasks that produce a specific service or product for customers. A process is where the work gets done, and value creation occurs through transforming input into output.

- ***Skills and Competencies***: Specialized skills that become part of the organizational core competency enable innovation and create a competitive edge. Organizations that invest in research and development which emphasize investing in people's training and well-being will shape a winning strategy.

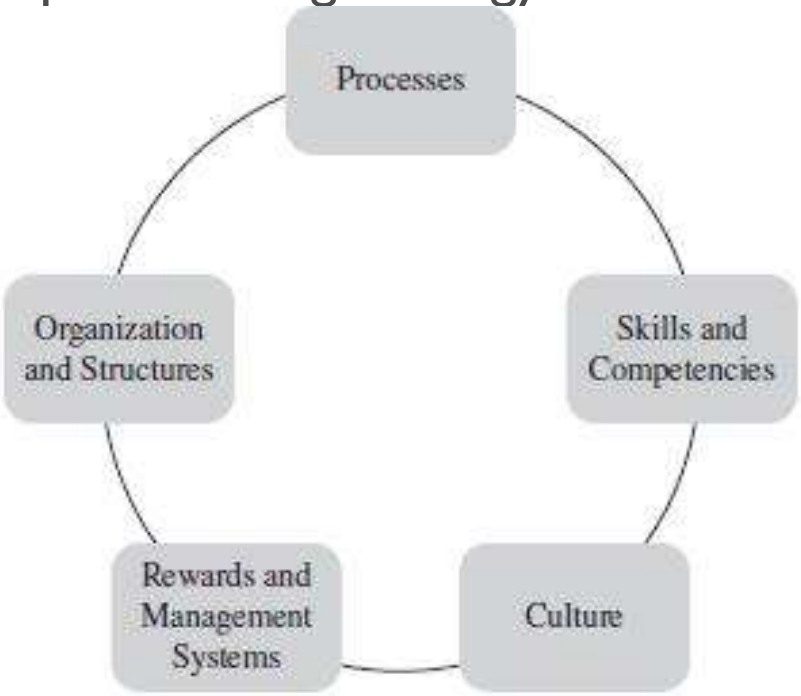


FIGURE 22.2. CROPS framework.

Change Management Maturity model (CMMM)

- A Change Management Maturity Model (CMMM) helps organization to analyze, understand, and visualize the strength and weakness of the firm's change management process and identify opportunities for improvement and building competitiveness.
- The model should be simple enough to use and flexible to adapt to different situations
- The business value of CMMM can be expressed in terms of improvements in business efficiency and effectiveness. All organizational investments are business investments, including IT investments. The resulting benefits should be measured in terms of business returns.
- Therefore CMMM value can be articulated as the ratio of business performance to CMMM investment;

- ROIT (CMMM) = Estimated Total business performance improvement

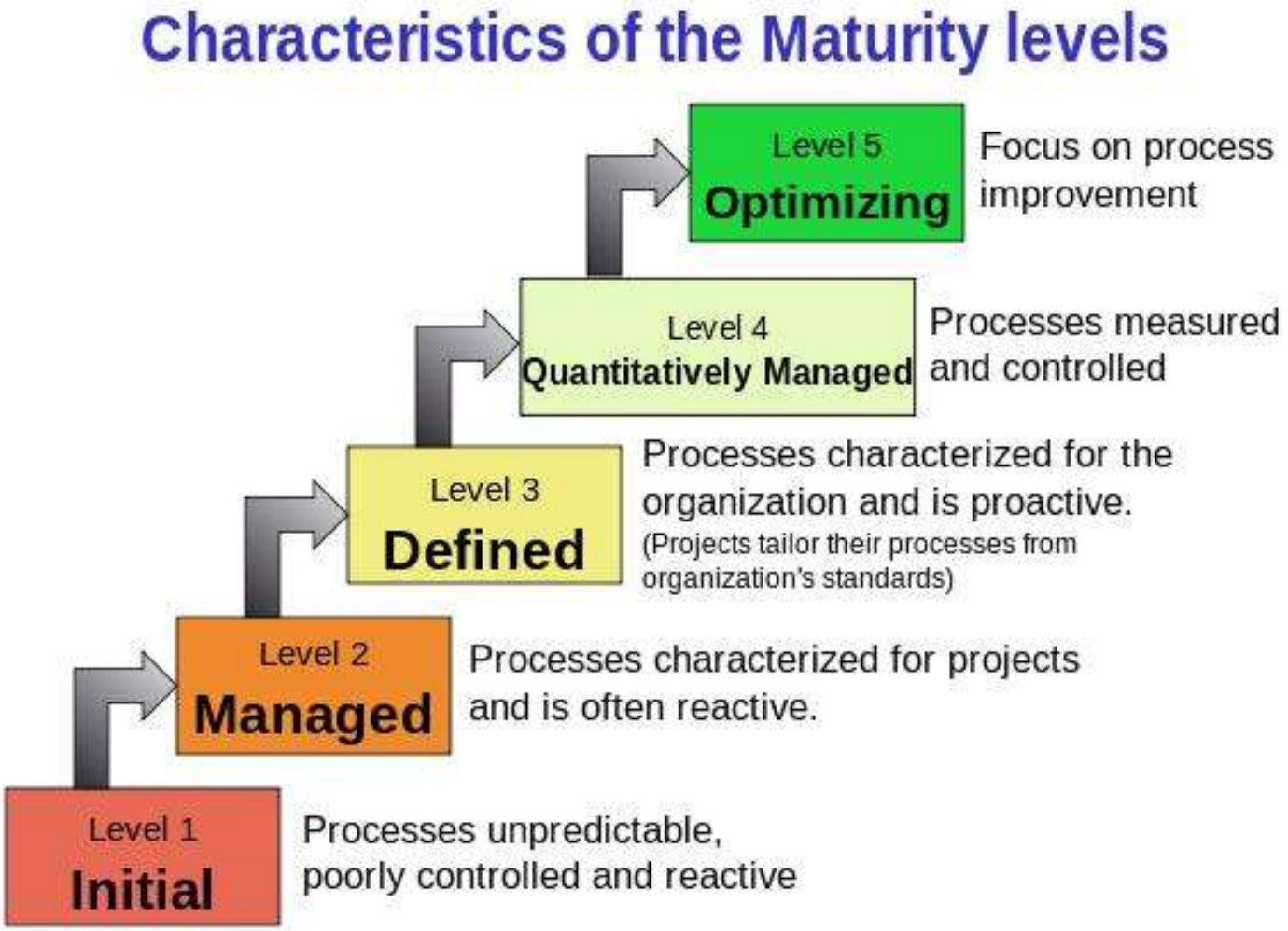
  ---

  Total CMM investment (TCO)

Where,

- ROIT : Obeserved business value or total return on investment from IT initiative (CMMM)
- Business performance improvement – Reduce error rate
- Increase cutomer/user satisfaction – customer and employee retension
- Increase market share and revenue
- Increase sales from existing customer
- Improve productivity
- CMMM investment – initial capital investment and total cost of ownership over the life of investment

CMM levels


Characteristics of the Maturity levels
Level 5
Optimizing
Focus on process improvement
Level 4
Quantitatively Managed
Processes measured and controlled
Level 3
Defined
Processes characterized for the organization and is proactive.
(Projects tailor their processes from organization's standards)
Level 2
Managed
Processes characterized for projects and is often reactive.
Level 1
Initial
Processes unpredictable, poorly controlled and reactive

Organizational Readiness self-assessment: (Who, When, Where and How)

- An organizational assessment is a process intending to seek a better understanding of *as-is (current)* state of the organization.
- It also defines the roadmap required to fill the gap and to get the organization moving toward where it wants to go.
- The process implies that the organization needs to complete the strategy analysis process first and to formulate the future goals.
- The assessment can be conducted by either an internal or external professional. During the effective organization readiness assessment, it is desirable to achieve following:
  - Articulate and reinforce the reason for change.
  - Determine the as-is state
  - Identify gap between future and current state
  - Assess barriers to change
  - Establish action plan to remove barriers.

- It is also important to select the right people for the assessment across the organization.
- Asking right questions is also essential. The assessment should provide insight into your challenges and help determine some of the key questions that need to be asked.

Data security in the Cloud

Introduction

- Security is very important in every aspect, whether it is real world or digital world.
- Even the information under the lock and key is subject to theft or uncertainty or accidental or misuse.
- Even in the digital world, if the data information is in encrypted form, still there are evidence of losses.
- This has become more evident as era of cloud computing has come.
- Information in the cloud environment has much more dynamism and fluidity than information that is static on a desktop or in a network folder.

The current state of data security in the cloud.

- Cloud computing offers many benefits in terms of data sharing and cost effectiveness, this is why most of the people use it, but on the other hand there are various people who are more concerned about the security and so are not willing to use it.
- The security issues began when focusing on the securing of access to the datacenters where the data resides. This is known that it does not cover the vast majority of the instances of data that are outside the confines of the data center.
- Different organizations and companies are having different ways of securing their data so that they are easily moved without any fear of loss.

Cloud computing and data security risk

- In cloud computing, the data is been stored and uploaded by the third party cloud provider, here there are various risks associated with it:
- Firstly, it is necessary to protect the data during upload into the data center to ensure that the data do not get hijacked on the way into the database.
- Secondly, it is necessary to store the data in the data center to ensure that they are encrypted at all times.
- Thirdly, and perhaps obvious the access to those data need to be controlled.
- This control should also be applied to the hosting company including the administrators of the data center.
- Other issues that complicate the area of hosted data include ensuring that the various data security acts and rules are adhered to.

- A further area of risk associated not only with cloud computing, but also with traditional network computing, is the use of content after access.
- The risk is potentially higher in a cloud network because the information is outside of your corporate walls.
- Compliance with data security directives and acts still needs to be met, no matter what platform for communication is being used.
- Leaking of sensitive information can affect the integrity of the data.
- Cloud computing more than any other form of digital communication technology, has created a need to ensure that protection is applied at the inception of the information ensuring that a security policy becomes an integral part of that data throughout its life cycle.

Cloud Computing and Identity

- Digital Identity holds the key to flexible data security within a cloud environment. This is taken by choice by a number of industry leaders.
- It is also one of the most difficult technological methods to get it right. Identity is perhaps the most closest to the heart of the individual as it represents who we are.
- Digital identity can be used to form the basis of data security, not only in the cloud but also at the local level too.
- Access, Identity and Risk are the three variables that can become inherently connected when applied to the security of data. As access increases, risk to the security of data increases.
- Ultimately, digital identity holds the key to securing data, if that digital identity can be programmatically linked to security policies controlling the post access usage of data.
- A digital identity can carry with it many identifiers about individual tht makes identity theft a problem, but identity should also be kept private for the simple reason of respect.

- Identity, Reputation and Trust
  - Digital Identity is less considered because it is the link between the identity and the reputation of the individual identity owner.
  - Reputation is a real-world commodity that is a basic requirement of human –to-human relationships.
  - Basic communication structure is built on the idea of reputation and the trust.
  - Reputation can be extremely useful when used with digital identity.
  - They can be used to associate varying levels of trust with that identity , which in turn can be used to define the level of security policy applied to data resources.

- Identity for Identity's Sake
  - In the cloud you may find that you need a different "identity" or set of identifiers to access resources or perform different tasks.
  - If digital identity is to be used as data security system , then it must be made sure that the identity layer of cloud computing is able to handle very flexible requirements of data security.
  - These include the need for free flow of information, dynamic policies, data-centric security, and privacy.

- Cloud Identity: User-Centric and Open Identity Systems.
  - As the use of the internet and cloud computing increases, risks associated with identifying yourself have also increased.
  - Indentify fraud and theft are a real threat to the acceptance of cloud computing.
  - Internet identities like, information cards were originally designed to over the problem of "password fatigue" which is increasing problem for users who needs to remember multiple log on credentials.
  - Similarly, OpenID was developed for the purpose of an easier logon into multiple web sites.

- The philosophy of User-Centric Identity
  - Digital identities are a still evolving mechanism for identifying an individual particularly with cloud environment.
  - But Identity ownership being placed upon the individual i.e. user-centric is formed.
  - This has many advantages that includes the potential to improve the privacy aspects of a digital identity, by giving an individual the ability to apply permission policies based on their identity.
  - The term user-centric means that an identity may be controllable by the end-user, to the extent that the user can then decide what information is given to the party relying in the identity.

- User-Centric but Manageable
  - Here the user-centric implies that the identity is under the control and management of the end user.
  - For, example in the case of many user-centric identities, the user can entirely create and mange them within their own desktop or cloud environment.
  - With the context of data security, a personally managed identity may not carry enough assurance.
  - User-centric identities can be under the user control and thus must be issued and managed by a trusted host who are able to verify the user.

- Information card
  - Information card permit a user to present to a website or other service one or more claims, in the form of a software token, which may be used to uniquely identify the user.
  - They can be used in place of user name/passwords, digital certificates, and other identification systems, when user identity needs to be established to control access to a web site or to permit digital signing.
  - Information cards are part of an identity meta-system consisting of:
    - 1) Identity providers (Idp) , who provision and manage information cards, with specific claims to users.
    - 2) Users who own and utilize the cards to gain access to web sites and other resources that support information cards.

- 3) An identity selector/service, which is a piece of software on the user's desktop or in the cloud that allows a user to select and manage their cards.
- 4) Relying parties, these are the applications, services that can use an information card to authenticate a person and to then authorize an action such as logging onto a web site, accessing a document, signing content and so on.

Each information card is associated with a set of claims which can be used to Identity the user. These claims include identifiers such as name, email address, post code and so on.

One of the positive aspects of an Information card is the user-centric nature of the card. An information card Idp can be set up so that the end users themselves can self-issue a card, based on the required claims that they themselves input.

- The weakness and strengths of Information card
  - The dynamic nature of information cards is the strengths of the system.
  - The methods used within is has drawbacks. There are various information card identity provisioning services on offer include, Microsoft Geneva, Parity, Azigo and Avoco secure. Each offers varying levels of card authentication and are chosen from username and password, token and digital certificate and personal card.
  - Username and passwords are less secure and also not transparent.
  - Digital certificates can be difficult for less technical users to install and use.

The Cloud, digital Identity and Data Security

- Data are most often information that needs to be used; it may be passed through various persons and for collaboration and completion and can end up for storage in data center.
- One aspect of data security we need to assess before embarking on creating a security model for data in the cloud is the levels of need.
- The levels of security of any data object should be thought of as concentric layers like :
  - Level 1: Transmission of the file using encryption protocols
  - Level 2: Access control to the file itself, but without encryption of the content
  - Level 3: Access control (including encryption of the content of the data object)
  - Level 4: Access Control (including encryption of the content of the data object) but also including rights management options like no copying, no printing etc.

- Other options that can be included in securing data also include watermarking or red-acting of content.
- The current state of cloud computing gives us various types of models like public, private and hybrid cloud.
- The fluid movement of data through and between these clouds is an integral part of the cloud should be secure.

Content Level Security Pros and cons

- Data protected at the content level as certain advantages, like greater control, more focused access control, increased protection over content, and assurance within a cloud-hosted system.
- But there are problems when the data are transferred and need to be decrypted when need to be used or accessed every time. And it needs to secure or retain the protection of data within the structure of the database itself.

UNIT – 4
ORGANIZATIONAL READINESS AND CHANGE MANAGEMENT IN THE CLOUD AGE

PREPARED BY: PROF. DISHA H. PAREKH DOSHI

INTRODUCTION

- The studies for organization for economic co-operation and development (OECD) economics demonstrated that there is a strong correlation between changes in organization and workplace practices and investment in IT.
- In order to effectively enable and support enterprise business goals and strategies, it must adapt new technologies and continually change.
- Organization should have a transition to a desirable level of CMM (change management maturity) by having following key knowledge:
  - **Domain 1**: managing the environment, understanding the organization (people, process and culture)
  - **Domain 2**: recognizing and analyzing the trends (business and technology), observe the key driver for changes.
  - **Domain 3**: leading for results, assess organizational readiness and architect solution that delivers definite business values.

BASIC CONCEPT OF ORGANIZATIONAL READINESS

- People in the organization face the change as challenging. They have fear or uncertainties. This is called FUD syndrome: Fear, Uncertainty and Doubt.
- Employees are used to with their roles and responsibility and are familiar with their environment and management's expectations.
- But when corporate changes are made, it is common that people tend to become uncomfortable and excited regardless the level and intensity of change.

DRIVERS FOR CHANGES: A FRAMEWORK TO COMPREHEND THE COMPETITIVE ENVIRONMENT

- The five driving factors for change given by the framework are:

1. **Economic (global and local, external and internal)**
    - Economic factors are usually dealing with the state of economy, both local and global in scale. Managers and groups are expected to deal with the unpleasant facts of shrinking market share, declining profit margins, unsatisfactory earnings, new and increasing competition. Managers are often asked to do more with less, and this is done during downturn.
2. **Legal, political, and regulatory compliance**
    - This deals with issues of transparency, compliance and conformity. The objective is to be a good corporate citizen and industry leader and to avoid the potential cost of legal threats from external factors.
3. **Environmental (industry structure and trends)**
    - Environmental factors usually deal with the quality of natural environments, human health, and safety.
4. **Technology developments and innovation**
    - New technologies and innovations everywhere has played very important part and has changed the lives of so many fields.
5. **Socio cultural (markets and customers)**
    - It sees the societal expectations and trends and how cloud computing change the world of markets and customers.

COMMON CHANGE MANAGEMENT MODELS

1) Lewin's Change Management Model

- Kurt Lewin, a psychologist by training, observed that there are three stages of changes, which **are Unfreeze, Transition and Refreeze.**
- It is recognized that people tend to become comfortable in this freeze or unchanging environment and they wish to remain in this safe/comfort zone. Any disturbance to them will make them uncomfortable.
- To encourage change, its necessary to unfreeze the environment by motivating people to accept the change. Motivation for change must be generated before change can occur. This is the unfreezing stage from which change begins.
- The transition phase is when the change plan is executed and actual change is being implemented.
- The last phase is Refreeze, this is the stage when the organization once becomes unchanging/frozen until the next time a change is initiated.

COMMON CHANGE MANAGEMENT MODELS

2) Deming Cycle(Plan, Do, Check, Act)

- The Deming cycle is also known as the **PDCA cycle**.
- It is a continuous improvement model with four sequential sub processes: Plan, Do, Check and Act.
- The PDCA cycle is usually implemented as an evergreen process, which means that the end of one complete cycle or pass flows into the beginning of the next pass and thus supports the concept of continuous quality improvement.
- **PLAN : Recognize an opportunity and plan a change.**
- **DO : Execute the plan in a small scale to prove the concept.**
- **CHECK :Evaluate the performance of the change and report the results to sponsor.**
- **ACT : Decide on accepting the change and standardizing it as a part of the process.**

A PROPOSED WORKING MODEL : CROPS

- CROPS framework is a working model which stands for **Culture, Rewards, Organization and Structures, Process, Skills and Competencies**
- **Culture :**
  - Corporate culture is a reflection of organizational (management and employees) values and belief.
  - The culture of a group can be defined as, A pattern of shared basic assumptions that the group learned as it solved its problems of external adaption and internal integration, that has worked well enough to be considered valid and therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems.
- **Rewards and Management System :**
  - This management system focuses on how employees are trained to ensure that they have the right skills and tools to do the right job. It identifies how to measure employee job performance and how company compensates them based on their performance. Reward is the most important that shapes employees values and beliefs.
- **Organization and Structures :**
  - How the organization is structured is largely influenced by what the jobs are and how the jobs are performed. Business processes need to align with organizational vision, mission, and strategies in order to create customer and shareholder values.
- **Process :**
  - Business process or business method as a collection of related, structured activities or tasks that produce a specific service or product for customers. A process is where the work gets done, and value creation occurs through transforming input into output.
- **Skills and Competencies:**
  - Specialized skills that become part of the organizational core competency enable innovation and create a competitive edge. Organizations that invest in research and development which emphasize investing in people's training and well-being will shape a winning strategy.

A PROPOSED WORKING MODEL : CROPS

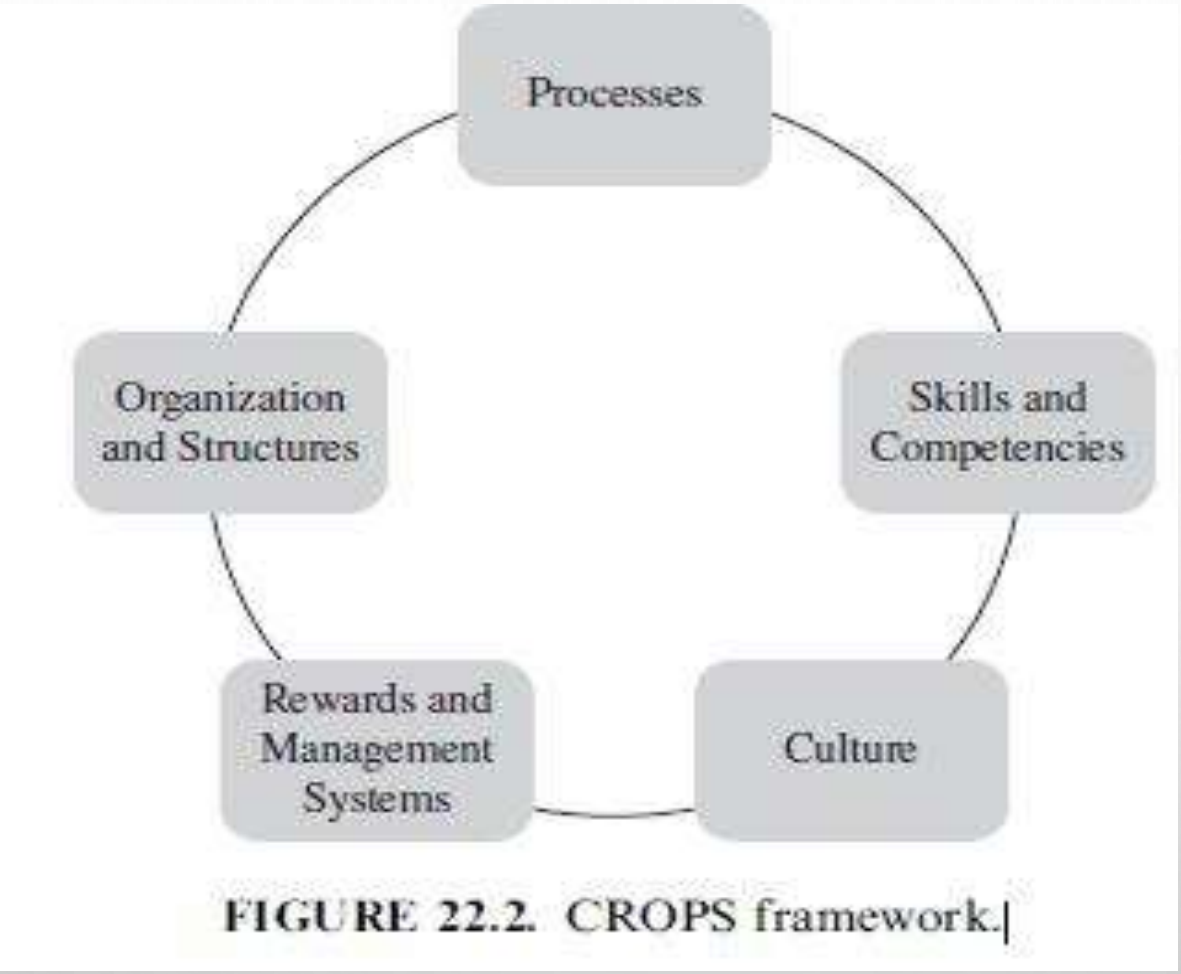


FIGURE 22.2. CROPS framework.

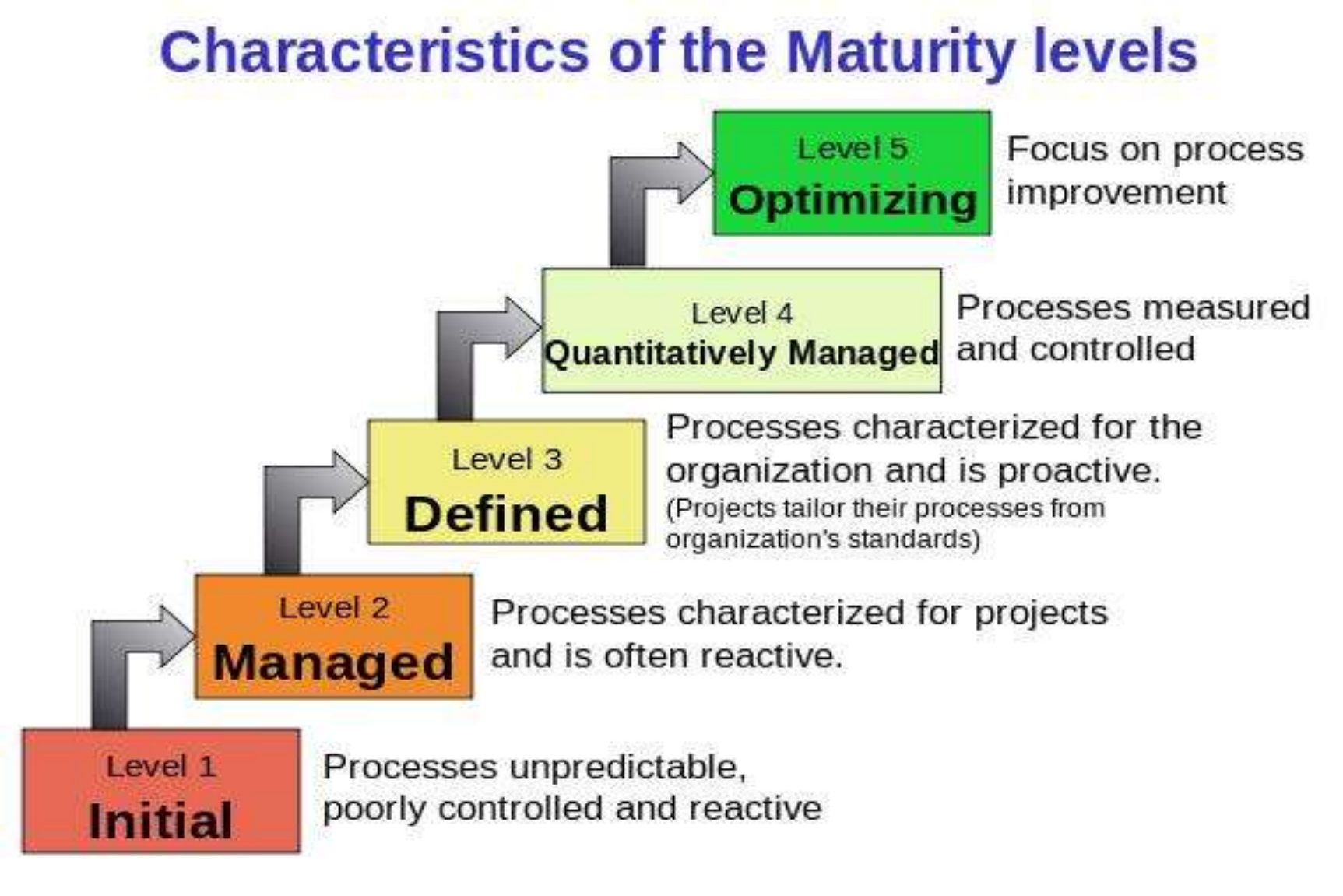
CHANGE MANAGEMENT MATURITY MODEL (CMMM)

- A Change Management Maturity Model (CMMM) **helps organization to analyze, understand, and visualize the strength and weakness of the firm's change management process and identify opportunities for improvement and building competitiveness.**
- The model should be simple enough to use and flexible to adapt to different situations
- The business value of CMMM can be expressed in terms of improvements in business efficiency and effectiveness. All organizational investments are business investments, including IT investments. The resulting benefits should be measured in terms of business returns.
- Therefore CMMM value can be articulated as the ratio of business performance to CMMM investment:
- ROIT (CMMM) = Estimated Total business performance improvement

$$\frac{\text{Estimated Total business performance improvement}}{\text{Total CMM investment (TCO)}}$$

- Where,
  - ROIT : Observed business value or total return on investment from IT initiative (CMMM)
  - Business performance improvement – Reduce error rate
  - Increase customer/user satisfaction – customer and employee retention
  - Increase market share and revenue
  - Increase sales from existing customer
  - Improve productivity
  - CMMM investment – initial capital investment and total cost of ownership over the life of investment

CMM LEVELS


Characteristics of the Maturity levels
Level 5
Optimizing
Focus on process improvement
Level 4
Quantitatively Managed
Processes measured and controlled
Level 3
Defined
Processes characterized for the organization and is proactive.
(Projects tailor their processes from organization's standards)
Level 2
Managed
Processes characterized for projects and is often reactive.
Level 1
Initial
Processes unpredictable, poorly controlled and reactive

UNIT – 4
DATA SECURITY IN THE CLOUD

INTRODUCTION

- Security is very important in every aspect, whether it is real world or digital world.
- Even the information under the lock and key is subject to theft or uncertainty or accidental or misuse.
- Even in the digital world, if the data information is in encrypted form, still there are evidence of losses.
- This has become more evident as era of cloud computing has come.
- Information in the cloud environment has much more dynamism and fluidity than information that is static on a desktop or in a network folder.

CLOUD COMPUTING AND DATA SECURITY RISK

- In cloud computing, the data is been stored and uploaded by the third party cloud provider, here there are various risks associated with it:
- Firstly, it is necessary to protect the data during upload into the data center to ensure that the data do not get hijacked on the way into the database.
- Secondly, it is necessary to store the data in the data center to ensure that they are encrypted at all times.
- Thirdly, and perhaps obvious the access to those data need to be controlled.

CLOUD COMPUTING AND IDENTITY

- In cloud computing, the data is been stored and uploaded by the third party cloud provider, here there are various risks associated with it:
- Firstly, it is necessary to protect the data during upload into the data center to ensure that the data do not get hijacked on the way into the database.
- Secondly, it is necessary to store the data in the data center to ensure that they are encrypted at all times.
- Thirdly, and perhaps obvious the access to those data need to be controlled.
- Access, Identity and Risk are the three variables that can become inherently connected when applied to the security of data. As access increases, risk to the security of data increases.
- Ultimately, digital identity holds the key to securing data, if that digital identity can be programmatically linked to security policies controlling the post access usage of data.
- A digital identity can carry with it many identifiers about individual that makes identity theft a problem, but identity should also be kept private for the simple reason of respect.

IDENTITY, REPUTATION AND TRUST

- Digital Identity is less considered because it is the link between the identity and the reputation of the individual identity owner.
- Reputation is a real-world commodity that is a basic requirement of human –to-human relationships.
- Basic communication structure is built on the idea of reputation and the trust.
- Reputation can be extremely useful when used with digital identity.
- They can be used to associate varying levels of trust with that identity , which in turn can be used to define the level of security policy applied to data resources.

CLOUD IDENTITY: USER-CENTRIC AND OPEN IDENTITY SYSTEMS.

- As the use of the internet and cloud computing increases, risks associated with identifying yourself have also increased.
- Identify fraud and theft are a real threat to the acceptance of cloud computing.
- Internet identities like, information cards were originally designed to overcome the problem of “password fatigue” which is increasing problem for users who needs to remember multiple log on credentials.
- Similarly, OpenID was developed for the purpose of an easier logon into multiple web sites.

THE CLOUD, DIGITAL IDENTITY AND DATA SECURITY

- Data are most often information that needs to be used; it may be passed through various persons and for collaboration and completion and can end up for storage in data center.
- One aspect of data security we need to assess before embarking on creating a security model for data in the cloud is the levels of need.
- The levels of security of any data object should be thought of as concentric layers like :
- **Level 1: Transmission of the file using encryption protocols**
- **Level 2: Access control to the file itself, but without encryption of the content**
- **Level 3: Access control (including encryption of the content of the data object)**
- **Level 4: Access Control (including encryption of the content of the data object) but also including rights management options like no copying, no printing etc.**

ANEKA

- PaaS offer the right tools to implement and deploy hybrid clouds.
- It provide enterprises with a platform for creating, deploying, and managing distributed applications on top of existing infrastructures.
- There are so many different implementations of the PaaS model, Manjrasoft Aneka is one of them.
- Aneka is a programming and management platform for building and deploying cloud computing applications.

What is ANEKA?

- Aneka is a software platform and a framework for developing distributed applications on the cloud.
- It provides developers with a rich set of APIs for transparently exploiting these resources by expressing the application logic with variety of programs.
- Aneka, which is both a commercial solution and a research platform, positions itself as a Platform-as-a-Service implementation.
- Aneka provides not only a software infrastructure for scaling applications but also a wide range of APIs that help developers to design and implement applications.

- Developers can express distributed applications by using the API contained in the SDK or by porting existing legacy applications to the cloud.
- Such applications are executed on the Aneka cloud, represented by a collection of nodes connected through the network hosting the Aneka container.
- The container is a building block of middleware & represents the runtime environment for executing applications, it contains the core functionalities of the system and is built up from an extensible collection of services that allow administrators to customize the Aneka Cloud.

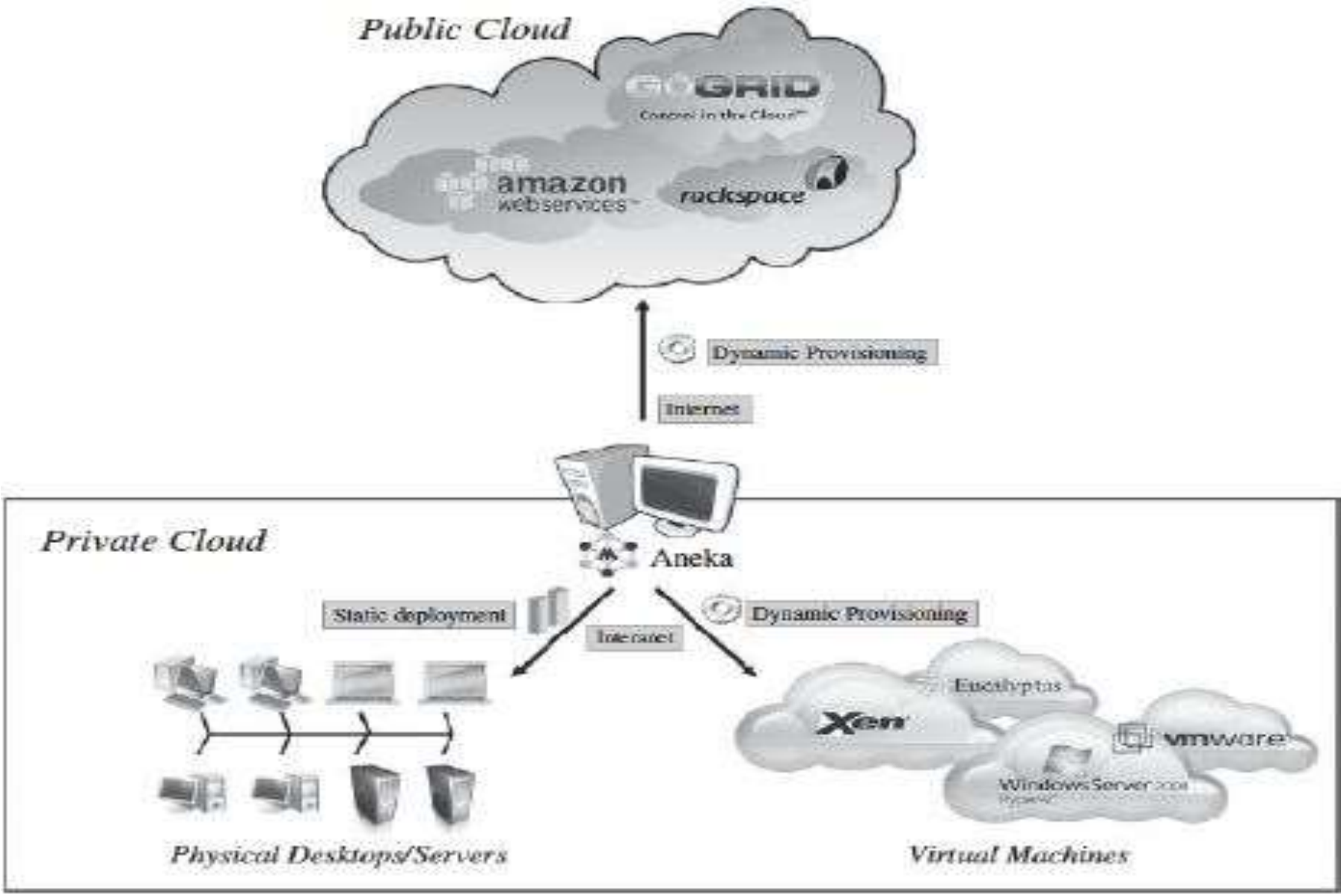
ANEKA CLOUD PLATFORM

- There are three classes of services that characterize the container:
  - ***Execution Services*** :They are responsible for scheduling and executing applications. Each of the programming models supported by Aneka defines specialized implementations of these services for managing the execution of a unit of work defined in the model.
  - ***Foundation Services:*** These are the core management services of the Aneka container. They are in charge of metering applications, allocating resources for execution and keeping the service registry updated.
  - ***Fabric Services****:* Constitute the lowest level of services stack of Aneka and provide access to resources managed by cloud. An important service in this layer is Resource Provisioning service.

ANEKA RESOURCE PROVISIONING SERVICE

- The most significant benefit of cloud computing is the elasticity of resources, services, and applications, which is the ability to automatically scale out based on demand and users quality of service requests.
- Applications managed by the Aneka container can be dynamically mapped to heterogeneous resources, which can grow or shrink according to the application's needs.
- This elasticity is achieved by means of the resource provisioning framework, which is composed of primarily of services built into the Aneka fabric layer.

Aneka resource provisioning over private and public clouds.



- The figure shows an overview of Aneka resource provisioning over private and public clouds. It combines privately owned resources with public rented resources to dynamically increase the resource capacity to a larger scale.
- Private resources identify computing and storage elements kept in the premises that has internal security and administrative policies.
- Aneka identifies two types of private resources: static and dynamic resources.
- Static resources are constituted by existing physical workstations and servers that may be idle for a certain period of time. Their membership to Aneka cloud is manually configured by admins and does not change.
- Dynamic resources are mostly represented by virtual instances that join and leave the Aneka cloud and are controlled by resource pool managers that provision and release them when needed.

Comet Cloud - An Autonomic Cloud Engine

Prof. Disha H. Parekh

Introduction

- Clouds have ***dynamic demand*** for resources and dynamic heterogeneous workloads.
- Eg, there is one application to be executed and it has 5 different tasks within it. Each task may dynamically need different types of resources or may be different number of resources.
- Some tasks may need high speed resources and some may not.
- This way there may be different applications with different tasks within it and each application may have different QOS requirements.

- May be one application need ***high throughput*** and other application is ***constrained by the budget*** and other may have to ***balance both***.
- Depending upon these different needs, the performance of cloud can also differ based on these varying loads and failures or network conditions and so on.
- *Combining the public cloud platform and integrating them with existing data centers* can support on-demand scale-up and scale-down and scale-out.
- Users may want to use resources in their private cloud i.e. Data centers first before scaling out into a public cloud, or they may have preference for particular cloud or may need to combine multiple clouds. Such integration and interoperability is currently non-trivial.
- ***CometCloud tries*** to provides such solution.

CometCloud

- CometCloud is an ***autonomic framework*** that is a virtual computational cloud which has a ***resizable computing capability.***
- CometCloud provides:

1. Infrastructures services for dynamic partnership and coordination to enable on-demand scale-up, scale-down and scale-out.
2. Programming support to enable a range of programming models and services for autonomic monitoring and management of the infrastructure and applications.

- It provides policy-based autonomic cloudbridging and cloudbursting.

- Cloudbridging: Autonomic cloudbridging enables ***on-the-fly integration*** of local computational environments(data centers, grids) and public cloud services like Amazon EC2 and Eucalyptus.

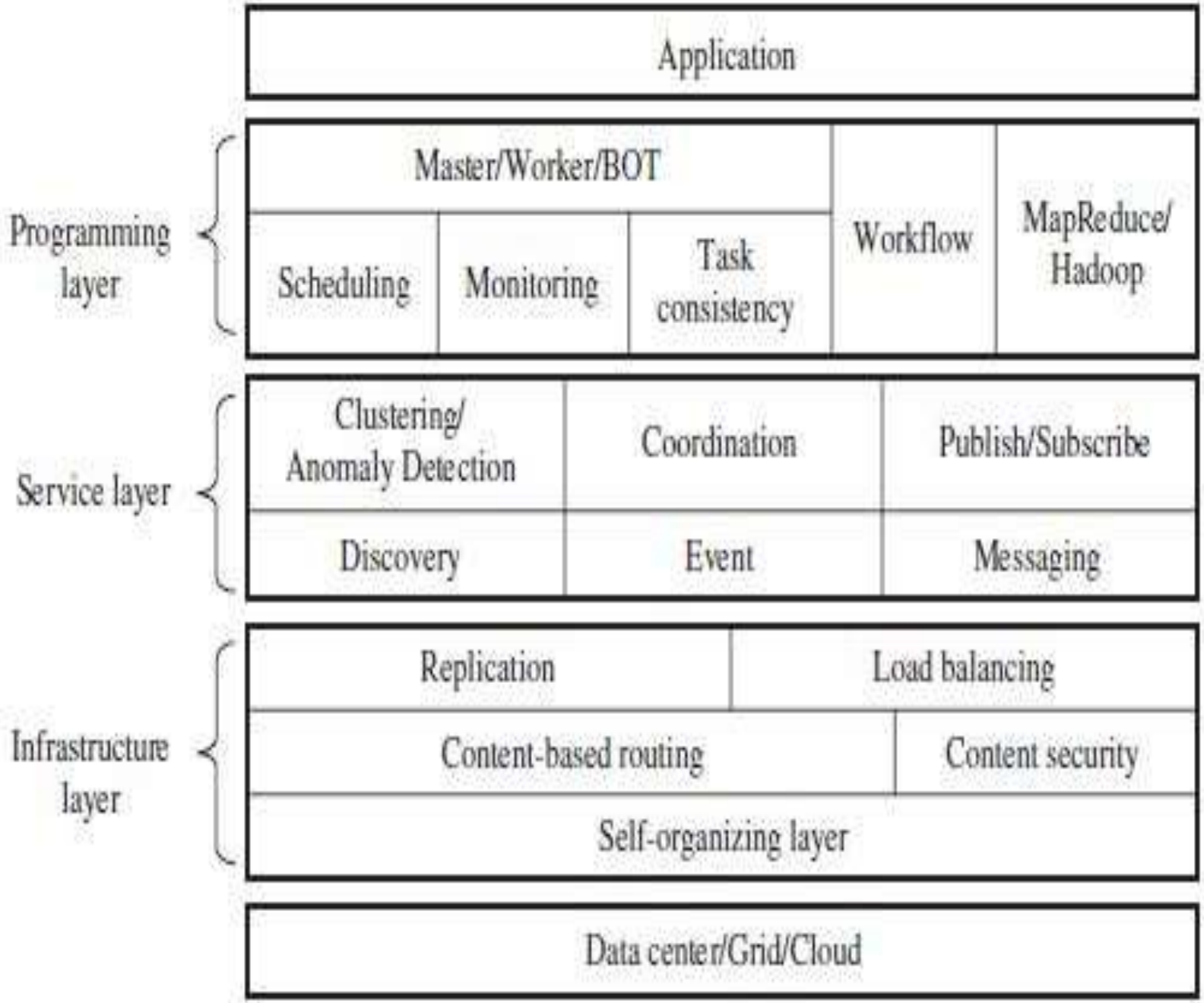
- Cloudbursting: Autonomic cloudbursting enables ***dynamic application scale-out*** to address dynamic workloads, spikes in demands, and other extreme requirements.

- CometCloud is based on a decentralized coordination substrate, and it supports highly heterogeneous and dynamic cloud/grid infrastructures, integration of public/private clouds, and cloudbursts.

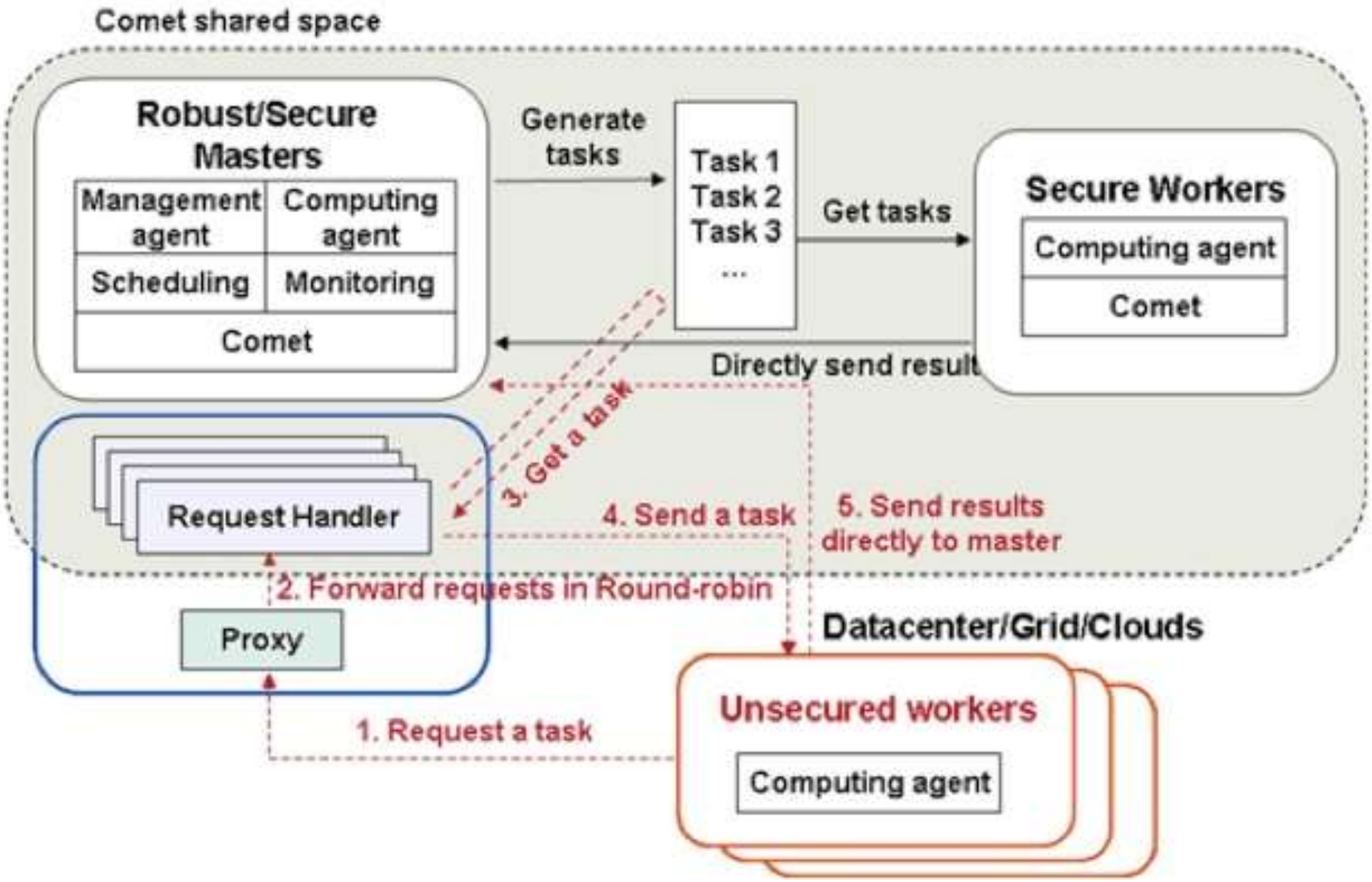
- CometCloud supports the dynamic requirements of real applications and multiple application groups with different computational requirements and QOS constraints.

COMETCLOUD ARCHITECTURE

- CometCloud is an autonomic computing engine for cloud and grid environments.
- CometCloud is based on peer-to-peer substrate that can span or extent enterprise data centers, grids and clouds.
- Resources can be assimilated or integrated on-demand and on-the-fly into its peer-to-peer overlay to provide services to applications.
- Its architecture is composed of a Programming layer, a Service Layer and an Infrastructure Layer.

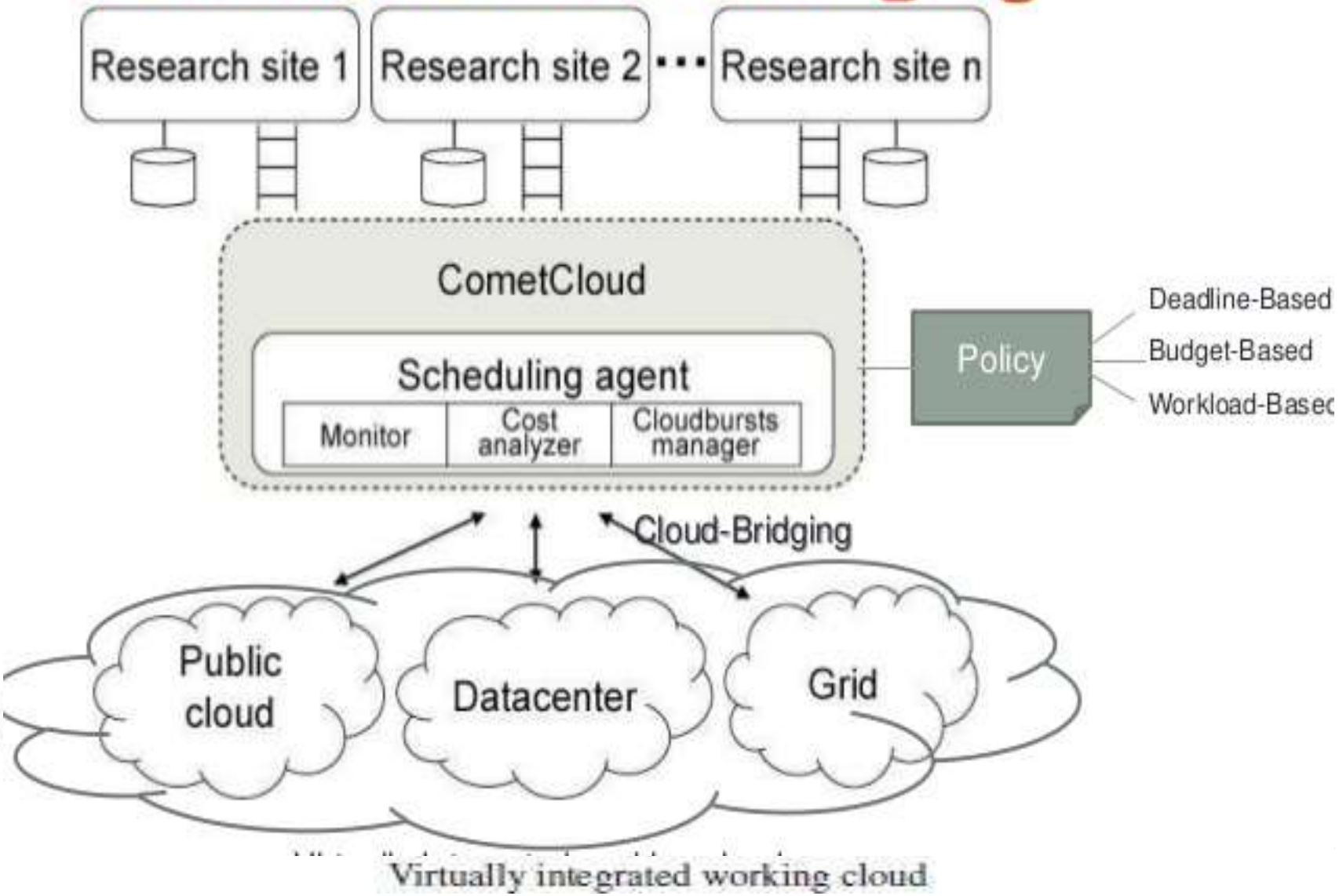

Application
Programming layer
Master/Worker/BOT
Scheduling
Monitoring
Task consistency
Workflow
MapReduce/ Hadoop
Service layer
Clustering/ Anomaly Detection
Coordination
Publish/Subscribe
Discovery
Event
Messaging
Infrastructure layer
Replication
Load balancing
Content-based routing
Content security
Self-organizing layer
Data center/Grid/Cloud

Autonomic Cloudbursting



- CometCloud considers ***three types of clouds*** based on perceived security/trust and assigns capabilities accordingly.
  - ***Master***
  - ***Secured Workers***
  - ***Unsecured Workers***
- If the space needs to be scale-up to store dynamically growing workload as well as requires more computing capability, then autonomic cloudbursts target secure worker to scale up. But only if more computing capability is required, then unsecured workers are added.

Automatic Cloudbridging



Contd

- Autonomic cloudbridging is meant ***to connect CometCloud and a virtual cloud*** which consists of public cloud, data center, and grid by the dynamic needs of the application.
- A ***scheduling agent manages autonomic cloudbursts*** over the virutal cloud, and there can be one or more scheduling agents.
- A scheduling agent is located at a robust/secure master site. If multiple collaborating research groups work together and each group requires generating tasks with its own data and managing the virtual cloud by its own policy, then it can have a separate scheduling agent in its master site.

- The ***requests*** for tasks generated by the different sites are ***logged in the CometCloud virtual shared space*** that spans master nodes at each of the sites.
- These tasks are then consumed by workers, which may run on local computational nodes at the site, a shared data center, grid or public cloud infrastructure.
- A scheduling agent manages QOS constraints and autonomic cloudbursts of its site according to defined policy.
- The workers can access the space using *appropriate credentials, access authorized tasks and return back results to the appropriate master* indicated in the task itself.

COntd

- We define ***three types of policies.***
- **Deadline-Based:-** When an application needs to be completed *as soon as possible*, assuming an adequate budget, the maximum required workers are allocated for the job.
- **Budget-Based:-** When a budget is enforced on the application, the number of workers allocated must ensure that the *budget is not violated*.
- **Workload-Based:-** When the application *workload changes, the number of workers* explicitly defined by the application is allocated or released.

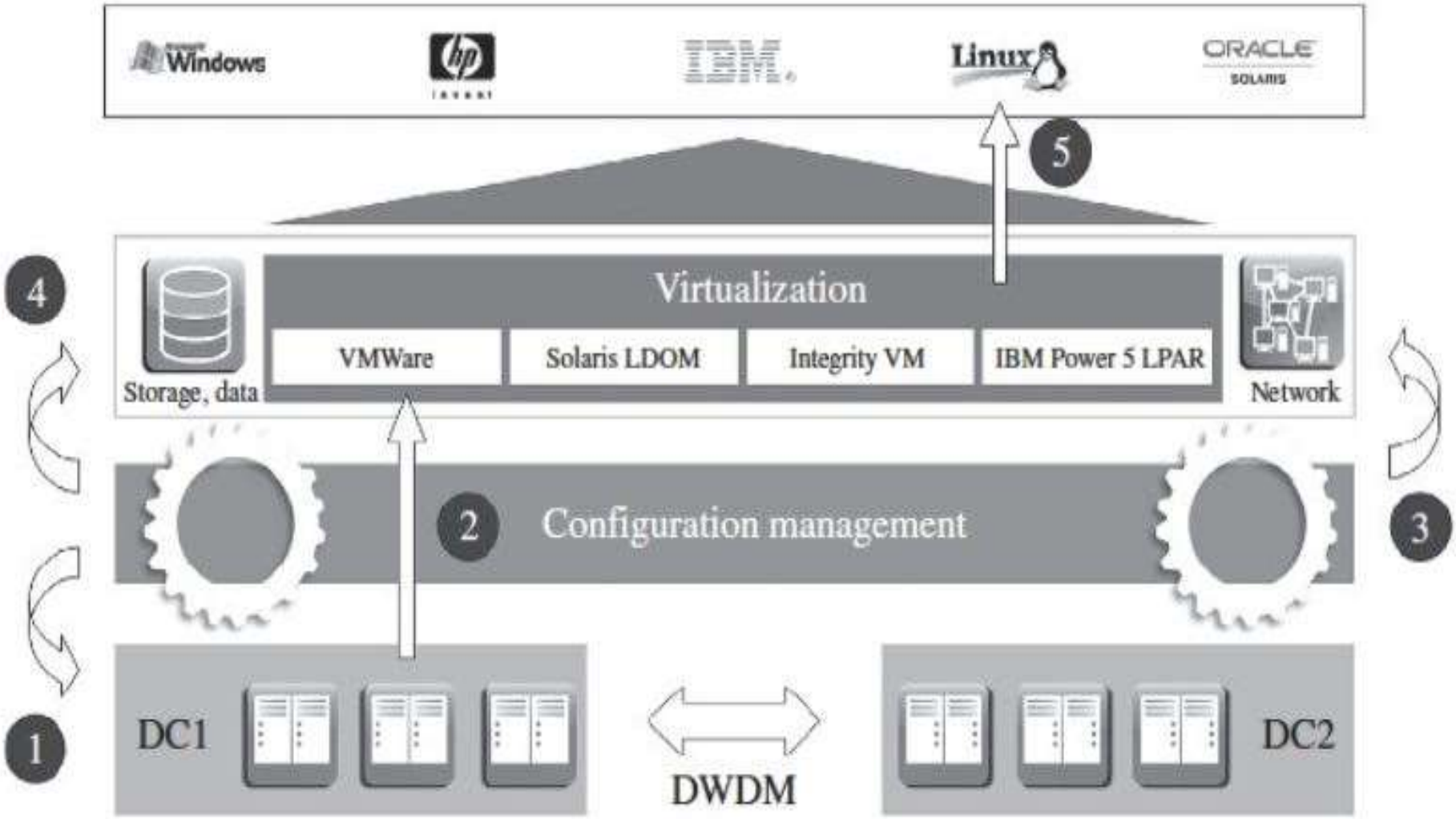
T-Systems' Cloud Based Solutions for Business Applications

Prof. Disha H. Parekh

Introduction

- T-Systems is one of the ***largest ICT service providers***, it offers a wide range of IT, telecommunications and integrated ICT services and has extensive experience in managing complex outsourcing projects.
- This company offers hosting and other services from its different data centers with over various servers at different places.
- It is a major provider of desktop and network services.
- T-systems approaches cloud computing from the viewpoint of an organization with an established portfolio of dynamic, scalable services delivered via network.

T systems' Core Cloud Modules



Computing

- The computing pool is based on server farms located in different data centers. Logical server systems are created automatically at these farms.
- The server systems are equipped with the network interface cards required for communication and integration with storage systems.
- The Configuration Management database (CMDB) plays a key role in computing resource pools. It selects and configures the required physical server (1).
- Once the server has been selected from the pool, virtualization technology is selected in line with the relevant application and needs (2).
- At the same time, configuration requirements are sent to the network configuration management system (3) and to the storage configuration management system (4).