Fundamental of Cloud Computing & Enterprise

Course Code IT413
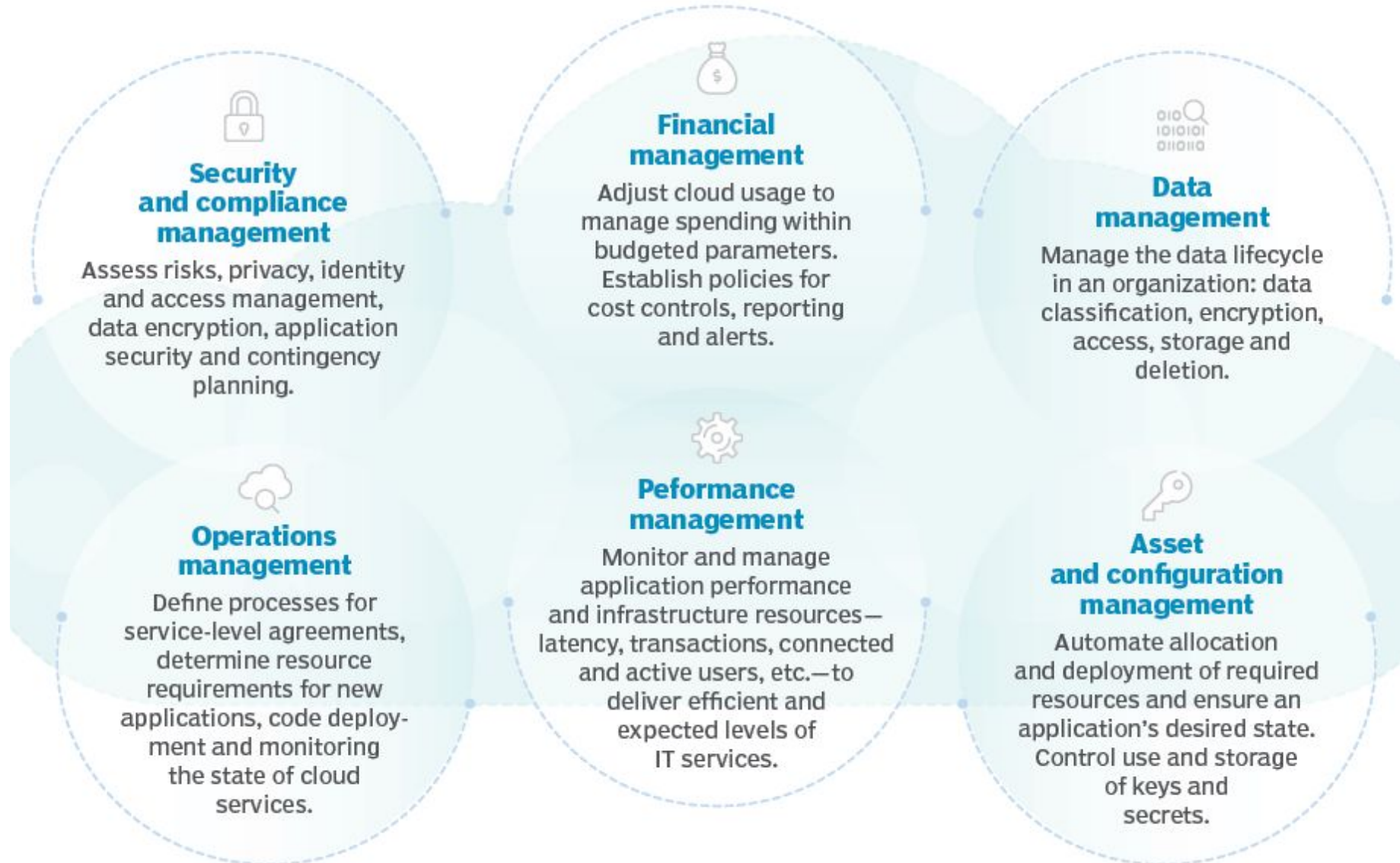*Module – III*
Topic – Brining Governance to the clouds

Prepared by
Dr. Seema Rawat
Deptt. of Information Technology and Engineering
Amity University Tashkent, Uzbekistan
Email- info@amity.uz

- People and processes
- Governance for the clouds
- Creating the Governance model: Define Polices, design Polices,
- Implement policies, Governance technology
- Governance technology.

Security and compliance management

Assess risks, privacy, identity and access management, data encryption, application security and contingency planning.

Financial management

Adjust cloud usage to manage spending within budgeted parameters. Establish policies for cost controls, reporting and alerts.

Data management

Manage the data lifecycle in an organization: data classification, encryption, access, storage and deletion.

Operations management

Define processes for service-level agreements, determine resource requirements for new applications, code deployment and monitoring the state of cloud services.

Peformance management

Monitor and manage application performance and infrastructure resources— latency, transactions, connected and active users, etc.—to deliver efficient and expected levels of IT services.

Asset and configuration management

Automate allocation and deployment of required resources and ensure an application's desired state. Control use and storage of keys and secrets.

- Many of the same security risks that companies face when dealing with their own computer systems are found in the cloud.

- With the cloud, we no longer have well-defined boundaries regarding what's internal and what's external to your systems. We must assess whether holes or vulnerabilities exist across servers, networks, infrastructure components, and endpoints and then continuously monitor them.

- According to the Cloud Security Alliance (CSA), an organization dedicated to ensuring security best practices in the cloud, significant areas of operational risk in the cloud include the following:

- Physical security: Covers security of IT equipment, network assets, and telecommunications infrastructure

- Human resource security: Deals with the people side of the equation — ensuring background checks, confidentiality, and segregation of duties (for example, those who develop applications don't operate them)

- Business continuity: Ensures that the provider meets its service level agreement for operation with you

- Disaster recovery: Ensures that your assets (your data and applications) are protected If, for example, you're using a public Infrastructure as a Service (IaaS) to run an application, find out what happens if there's some sort of disaster (natural or otherwise).

- Governance is about applying policies related to using services.

- Governance incorporates the organizing principles and rules that determine how an organization should behave when leveraging cloud services. These policies determine who is accountable for what actions.

- Cloud governance is a shared responsibility between the users of cloud services and the cloud provider.

- Understanding the boundaries of responsibilities and defining an appropriate governance strategy for a company requires careful balance.

- Identify and understand business objectives, determine high-level strategy and identify growth opportunities to realize how cloud technologies can help accelerate the growth.

- Develop an enterprise cloud computing strategy, including establishing key performance indicators (KPIs) to realize business goals. Involve stakeholders to ensure that the cloud computing strategy is fully aligned with organizational strategy and objectives.

- Review and map the cloud computing life cycle to existing enterprise processes and identify gaps that must be closed to meet the new cloud computing governance requirements.

- Prepare the necessary resources for the adoption of cloud computing. Align people, processes and technology, rationalize the current digital state, and address any skills gaps that would deter the use of new technologies.

- Ensure appropriate compliance review checkpoints are in place with the associated governing bodies.

- Refine existing governance bodies or define new governance bodies to carry out governance processes.

- Evolve governance processes along with business outcomes and metrics.

- The "people" refers to the human resources available at the firm's disposal. The people are the ones who do the tasks described in the process, sometimes by leveraging the technology.

- One of the main tasks is to onboard the right people. Businesses need to identify their key employees with the right skills, experience, and attitude for the job at hand. However, more often than not, key individuals are occupied or busy. Thus, the managers will have to wait for these right people to become available, hire new employees for the role, redirect people from other projects, or outsource the tasks to a consultant or agency. These are key decisions that are crucial to the success of the PPT framework impact.

- The Process

- A process is the steps or actions that combine to produce a particular goal. The process in the PPT framework mostly defines the "how" aspect. How will we achieve the desired result? How do we utilize the people and technology to solve the business problem? Processes are repeatable actions that theoretically produce the same result independent of who performs them.

- There are a few things to keep in mind while designing and implementing processes:

- Its imperative people understand how they fit into a process. They should understand the process, what their role is in it, and what they need to achieve. This means communicating the right instructions and training key people. They should be important stakeholders in the process design and review.

- Establishing a cloud governance program usually follows three basic phases:

- Awareness: Organizations in this stage have zero cloud structure and still depend on manual deployments of assets. They might know that they want to completely transition to the cloud, but they have minimal integrations and are just beginning to scope out cloud governance plans.

- Early Adoption: At this phase, organizations have developed policies matched to their particular processes. They likely have a cloud team in place and have scoped out costs and other architecture details. They are experiencing rapid cloud deployment.

- Mature Adoption: In this final phase, organizations reap the rewards of the effort they applied in the previous phases. Their cloud management is now fully automated. It is responsive and agile, and the cloud governance framework enhances security and compliance.

- Governance has a lot to do with assessing and managing risk. If you're going to hold a cloud provider (public, private, or hybrid) partly accountable for your IT cloud services, you need to consider risks.

- Governance team needs to consider the following risks:

- Audit and compliance: Include issues around data jurisdiction, data access control, and maintaining an auditing trail

- Security: Includes data integrity, confidentiality, and privacy

- Other information: Include protection of intellectual property

- Performance and availability: Include the level of availability and performance your business needs to be successful

- Interoperability: Associated with developing a service that may be composed of multiple services

- Contract: Associated with not reading in between the lines of your contract

- Billing: Associated with ensuring that you're billed correctly and only for the resources you consume

A typical IT governance model looks like the diagram below, and includes
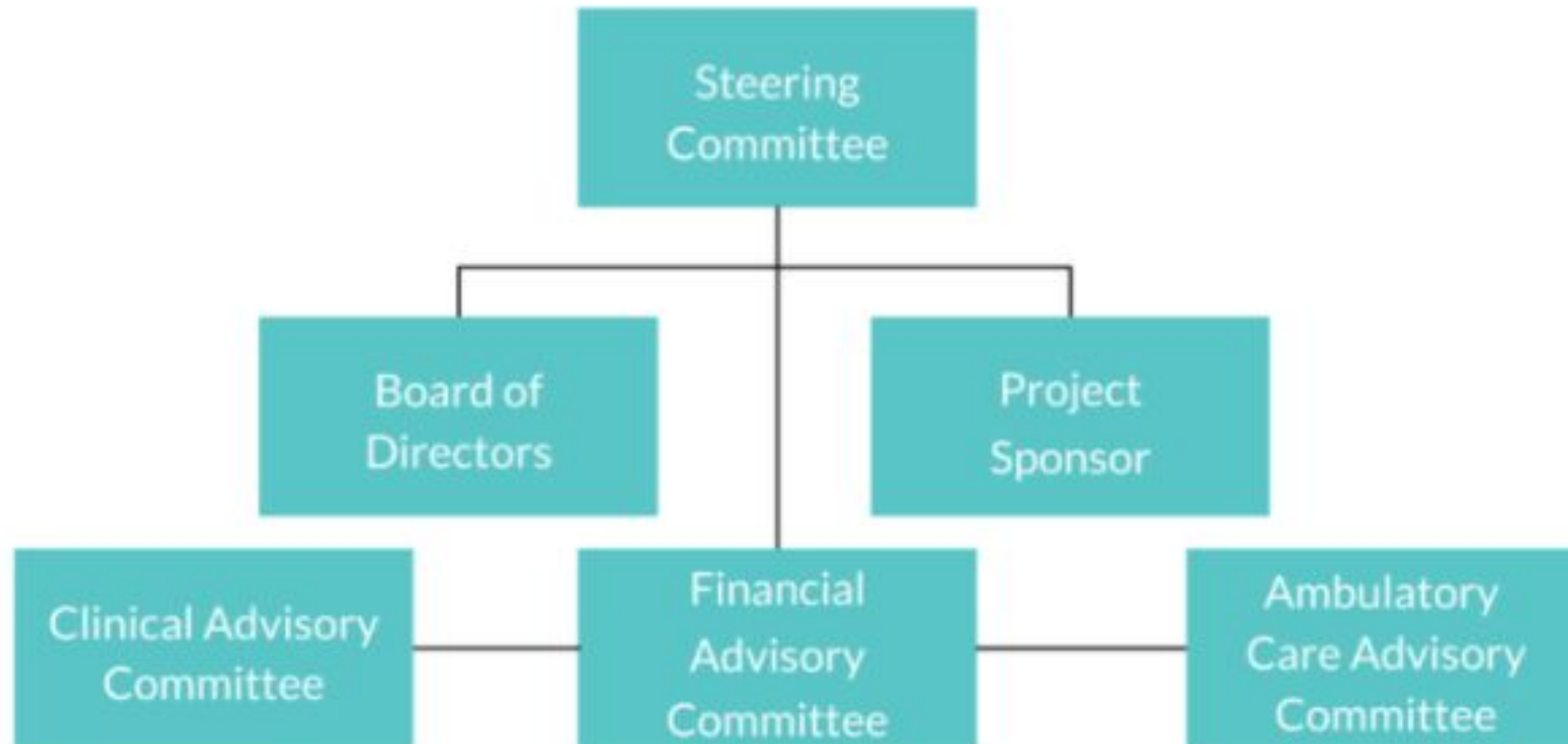
- What security policies does it have in place? Are they consistent with a recognized framework and control standard?

- Does the provider have any industry certifications?

- How does the provider meet audit standards?

- Does the service provider have documented policies and procedures, including escalation procedures in the event of an incident?

- How does the provider handle identity and access management?

- How does the provider protect data?

[1] https://cloudcomputing-news.net/news/2015/jan/15/how-cloud-providers-can-prevent-data-loss-guide/

[2] https://www.logikcull.com/blog/will-scotus-clarify-how-far-the-government-can-go-to-get-cloud-stored-data

[3] https://www.comparethecloud.net/opinions/data-loss-in-the-cloud/

Thank You