SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING(IoT and Cybersecurity Including BCT)

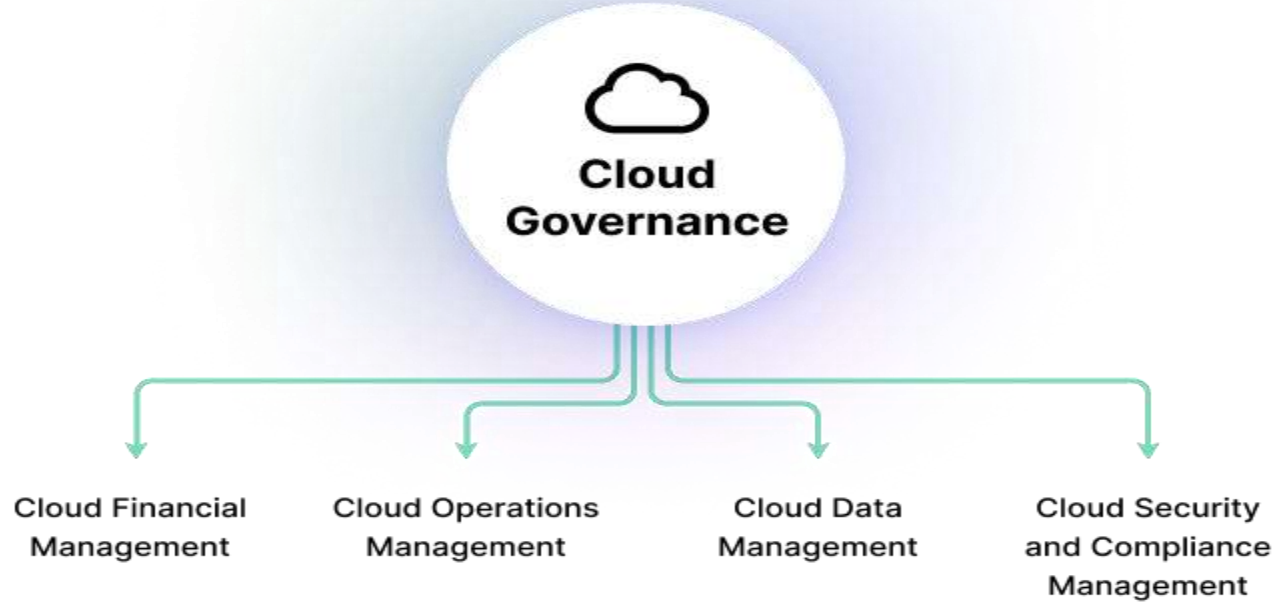
COURSE NAME : Cloud Service Management /19OE219

IV YEAR / VII SEMESTER

Unit II-

Topic : **Cloud Governance Framework**

How to Design and Implement a Cloud Governance Framework



Cloud Financial Management

In many organizations, cloud costs quickly get out of hand. Cloud services often promise to reduce IT costs, but this only holds true if costs are duly managed. There are three elements of cloud financial management:

- **Financial policies** clarifying how the organization plans to use the cloud. For example, policies can define in which cases managed services should be used to reduce in-house operating costs, or specify a cost management checklist that must be followed before deploying new cloud services.
- **Budgets** define the specific allowance for different parts of the organization or different categories of cloud services.
- **Cost reporting** is difficult to achieve in a consistent way. Some cloud services have unpredictable charges that can appear in different places of the cloud infrastructure—for example, cloud snapshots used for backup can be stored across different regions and accounts. You can use cost reporting tools provided by the cloud vendor, or adopt third party tools that cover multiple clouds.

Cloud Operations Management

Operations management involves defining processes for deployment of services. These processes should include:

- A clear definition of resources allocated to the service over time
- Service-level agreements (SLAs) to define expected performance
- Ongoing monitoring to make sure SLAs are met
- Process and required checks before deploying code to production
- Access control requirements

- Strong cloud operations management is an excellent way to prevent shadow IT. It can conserve costs by preventing unnecessary use of cloud resources, and can dramatically improve the return on investment of cloud expenditure in the long term.

Cloud Data Management

The cloud makes it easier to collect and analyze huge amounts of data, but this makes data management a much bigger challenge. Cloud governance should specify how to manage the entire data lifecycle in the cloud. This includes:

- Building a data classification scheme, and setting policies for data at different levels of sensitivity
- Ensuring all data is encrypted, at rest and in transit
- Putting in place appropriate access controls for each type of data
- Using data masking to reduce the risk of sensitive data when it is used for scenarios like development, testing, or training
- Developing a tiering strategy, moving data over time from high cost fast access systems to lower cost archival systems
- Ensuring that data lifecycle management is automated—this is critical to apply policies in large scale cloud deployments

Cloud Security and Compliance Management

Cloud governance takes responsibility for all the key topics of enterprise security. It determines what are the organization's security and compliance requirements, and ensuring they are enforced in the cloud environment:

- Risk assessment
- Identity and access management
- Data management and encryption
- Application security
- Disaster recovery

Cloud governance should strike a balance between business drivers and requirements, real security risks, and the requirements of compliance standards. It should use existing policies and security practices, extending them to the cloud and translating them to the cloud environment.