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 Service Model Risk Matrix

What is a cloud computing risk assessment?

- While the business benefits of cloud computing have gained much attention over the past few years, the security around it continues to worry managed service providers and IT staff.
- On-premise solutions may provide a feeling of more control, at least for the physical security of the company’s virtual infrastructure.
- With the cloud, that infrastructure is outsourced to a cloud service provider who may be hundreds, or even thousands, of miles away.
- MSPs can conduct a **cloud computing risk assessment matrix** to instill confidence in their clients.
- To help organizations understand the risks associated with certain cloud computing service providers, researchers from business, academia, government, and the non-profit sector have developed a range of risk assessments.
- These risk assessments help businesses make informed decisions on cloud computing service providers before they purchase a service.
- Some businesses may be willing to accept more risk for lower service costs, while other companies will want to maximize security every step of the way, depending on the overall mission of the business and the type of data that they want to protect.
- Companies that work with sensitive data whether its own intellectual property, information important to national security, or the personally identifiable information of its customers — will want high levels of security.

The guiding principles

By following these 10 principles from ISACA, MSPs can be confident that their cloud service provider is offering them the right service for their business. A loss of data can be incredibly costly to a business and, in some cases, even force closure. Following these safeguards will help ensure that businesses are in line with industry best practices.

Here are the 10 principles in more detail:

1. **Executives must have oversight.** Leaders must be vigilant in keeping the cloud and information assets safe, especially as the cloud security environment evolves over time.
2. **Management must take responsibility for cloud risks**. Namely, IT leadership must understand that the risks taken are their own and must evaluate the risks on an on-going basis.
3. **All requisite staff must know about the cloud.** Ignorance of IT is no longer allowed, and all stakeholders must know how the cloud works.
4. **Management must be aware of users.** Management should know who has access to cloud data and who can make changes and decisions.

5.**Management must authorize what the cloud is used for**. Management needs to be involved in giving approval for the specific purposes cloud technology should be used for.

6.**Sophisticated IT processes must be used.** While the cloud may be new, IT best practices live on and should be followed.

7.Management must invest in security. It's not enough to want security, but investments must be made to ensure data remains secure.

8.Management must foster compliance. Certain rules must be followed in order to use the cloud.

9.Management must continuously assess risk. Risk changes over time based on technology or business needs. Management must consistently reevaluate risk.

10.**Everyone must follow best practices.** Cloud computing features its own set of industry best practices, and they should be followed.