



SNS COLLEGE OF TECHNOLOGY



(An Autonomous Institution)

Re-accredited by NAAC with A+ grade, Accredited by NBA(CSE, IT, ECE, EEE & Mechanical)
Approved by AICTE, New Delhi, Recognized by UGC, Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER APPLICATIONS

COURSE

23CAE717
Cloud Computing

UNIT V

**Security in the
Cloud**

TOPIC

Risk Management-
Security Monitoring

Semester

II Semester /
I MCA



Process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes

- **risk analysis**
- **cost benefit analysis**
- **Selection**
- **implementation and test, security evaluation of safeguards, and**
- **overall security review**



- Misunderstanding



- Aiming for perfection



Not operational



Missing skilled, motivated
Human Resource



Risk Management (Security)



- ❑ Identification of technology assets;
- ❑ Identification of data and its links to business processes, applications, and data stores;
- ❑ Assignment of ownership and custodial responsibilities
- ❑ A formal risk assessment process should be created that allocates security resources linked to business continuity
- ❑ Owners have authority and accountability for information assets including
 - protection requirements, custodians implement confidentiality
 - Integrity, Availability
 - privacy controls

Risk Dimension in Cloud



Risk dimension	Deployment model		
	Private internal	Private external	Public
Data and regulatory	<ul style="list-style-type: none"> – Similar to traditional computing 	<ul style="list-style-type: none"> – Data leakage from a malicious insider – Unauthorized data access by the service provider – Lack of visibility into cloud operations and ability to monitor for compliance – Dependence on a service provider to ensure adequate internal controls 	<ul style="list-style-type: none"> – Data leakage from a malicious insider – Unauthorized data access by the service provider – Data leakage across shared infrastructure – Lack of flexibility for encryption, data control – Lack of visibility into cloud operations and ability to monitor for compliance – Dependence on a service provider to ensure adequate internal controls

Risk dimension	Deployment model		
	Private internal	Private external	Public
Technology	<ul style="list-style-type: none"> – Evolving technologies could require rearchitecture and/or retraining 	<ul style="list-style-type: none"> – Evolving technologies could require rearchitecture and/or retraining 	<ul style="list-style-type: none"> – Limitations on customization of service offerings – Compatibility with other cloud providers – Limited choice of technology and related tools
Operational	<ul style="list-style-type: none"> – Service reliability and uptime 	<ul style="list-style-type: none"> – Service reliability and uptime 	<ul style="list-style-type: none"> – Lack of service-level customization – Control over quality – Control over application availability and disaster recovery

Risk dimension	Deployment model		
	Private internal	Private external	Public
Vendor	<ul style="list-style-type: none"> – Similar to traditional computing 	<ul style="list-style-type: none"> – Association and reliance on a service provider 	<ul style="list-style-type: none"> – Association and reliance on a service provider
Financial	<ul style="list-style-type: none"> – Underestimating initial costs – Continuing to carry capital expenditures of hardware and software 	<ul style="list-style-type: none"> – Underestimating initial costs – In some cases, continuing to carry capital expenditures of hardware and software – Contract modification or cancellation fees – Additional overhead of managing service provider(s) 	<ul style="list-style-type: none"> – Contract modification or cancellation fees – Runaway costs from poor planning and periodic monitoring – Additional overhead of managing service provider(s)



Security Monitoring



- Centralized security information management systems
- integrate with network and other systems monitoring processes like (e.g., security information management, security event management, security information and event management, and security operations centers
- security threats and issues in application and data layers



References



- ❑ Kai Hwang, Geoffrey C Fox, Jack G Dongarra, “Distributed and Cloud Computing, From Parallel Processing to the Internet of Things”, Morgan Kaufmann Publishers, 2012
- ❑ James E. Smith, Ravi Nair, “Virtual Machines: Versatile Platforms for Systems and Processes”, Elsevier/Morgan Kaufmann, 2005.
- ❑ Kumar Saurabh, “Cloud Computing – insights into New-Era Infrastructure”, Wiley India, 2011.
- ❑ Toby Velte, Anthony Velte, Robert Elsenpeter, “Cloud Computing, A Practical Approach”, TMH, 2009.
- ❑ John W. Rittinghouse and James F. Ransome, “Cloud Computing: Implementation, Management, and Security”, CRC Press, 2011