CLOUD SERVICES

S Thenmozhi

Department of Computer Applications

CLOUD SERVICES

Cloud Application Design

S Thenmozhi

Department of Computer Applications

Risk Management

- Process of evaluating risks, deciding how are they to be controlled and monitored
- Suitable approaches for different domains
- Security procedures should not make difficult to use the system
- Trade-off between the cost and the security measure
- Risk Management Concepts
  - Follow standards – NIST, FIPS 200

- NIST - National Institute of Standards and Technology

  - Divides security controls in 3 categories – Technical, Operational and Management.

  - The controls in each category are further divided into 18 families. Eg: audit, accountability, response to failures etc

- FIPS 200 - Federal Information Processing Standards

  - Defines the security requirement as low-impact, moderate-impact or high-impact

  - Low-impact- limited degradation in capability if a security breach happens and system offers still the primary functions and most additional functions

  - Moderate impact – offers primary functions and less additional functions

  - High-impact – primary functions are not delivered

Risk Management Process

   1. Information Resource categorization

- Criticality – the impact to the business of a security failure.
- Sensitivity – confidentiality of the resource

   2. Select Security controls

- Whitelisting IP addresses. Making the administrators to work within office premises
- Specific registering for IPs from outside access

   3. Risk Assessment

- Anticipate threats and provide adequate protection against it

4. Implement Security Controls

- Implement controls on physical or virtual security system.

5. Operational monitoring – continuous monitoring

6. Periodic review – check whether the security controls are continued to be effective

- Any possibility of new threats and requirement for operational changes

THANK YOU

S Thenmozhi

Department of Computer Applications

thenmozhis@pes.edu

+91 80 6666 3333 Extn 393