Parul® University

Specialization - Cloud Computing - I

Prof. Dhruv Shah

Parul®
University

DIGITAL LEARNING CONTENT

Unit – 5

Cloud Risks and Cloud Security

Risks in cloud computing

Cloud computing offers computing resources as a service.

- **Cloud Service Providers (CSP)**: SaaS, PaaS.
- **Cloud Infrastructure Providers (CIP):** IaaS.
- Features: On-demand scalability, cost efficiency, and virtualization.

Levels of Cloud Computing

- **Infrastructure**: Server environments (IaaS).
- **Storage:** Databases, file storage services (Google BigTable, Amazon SimpleDB).
- **Platform:** Development environments (Ruby on Rails, LAMP, Django).
- **Application:** SaaS applications (Salesforce, Google Docs).
- **Services:** Web services, payment gateways (PayPal, Google Maps).
- **Client:** End users accessing cloud services via devices.

Risks in Cloud Computing

New and evolving risks due to virtualization and reliance on third-party providers.

Common risks:

- SLA violations.**Service Level Agreement (SLA)**
- Data security and privacy concerns.
- Vendor lock-in and compliance risks.
- Reduced control over infrastructure and software.
- Potential provider shutdowns.

Major Security Concerns

Secure data transfer: Encryption and authentication.

Secure application interfaces: API security.

Secure stored data: Data encryption and backups.

User access control: Role-based access management.

Data separation: Multi-tenancy risks and isolation.

Cloud ROI and Business Risks

- Risk #1: Economic feasibility – ROI must justify investment.
- Risk #2: Organizational challenges – Adoption must align with company culture.
- Risk #3: Integration difficulties – Compatibility with existing systems.
- Risk #4: Disaster recovery – Unforeseen failures must be mitigated.

Parul® University

DIGITAL LEARNING CONTENT

Risks in Cloud Computing: Cloud Impact

On IT Operations

- Reduced capital expenditure and operational costs.
- Shift from in-house infrastructure to cloud service providers.
- Increased agility in deploying and scaling IT resources.

On Business

- Faster innovation cycles due to scalable infrastructure.
- Risk of data loss and regulatory non-compliance.
- Potential cost savings versus hidden long-term expenses.

Security Concerns

- Risk of data breaches and cyber-attacks.
- Ensuring proper authentication and access control.
- Shared responsibility model with cloud providers.

Enterprise-Wide Risk Management

A structured approach to identifying, assessing, and mitigating risks.

Ensures business continuity and regulatory compliance.

Risk Management Process:

- 1. Determine objectives - Align risk management with business goals.
- 2. Identify risks - Recognize internal and external risks.
- 3. Evaluate risks - Assess potential impact and likelihood.
- 4. Select risk treatment - Mitigation, acceptance, transfer, or avoidance.
- 5. Implement decisions - Deploy security measures and policies.
- 6. Review and refine processes - Continuously improve risk strategies.

Types of Risks in Cloud Computing

Misuse and Illicit Use

- Attackers exploiting cloud resources for malicious activities.
- Hosting of illegal content or botnet operations.

Insecure Interfaces and APIs

- Poorly designed authentication mechanisms.
- Risk of API-based attacks leading to unauthorized access.

Insider Threats

- Employees misusing privileged access.
- Insider data theft or unintentional misconfigurations.

Types of Risks in Cloud Computing-Cont

Technology Sharing Risks:

- Vulnerabilities in multi-tenant architectures.
- Poor isolation leading to unauthorized access to shared resources.

Data Loss or Leakage:

- Accidental deletion, corruption, or unencrypted storage.

Account Hijacking:

- Phishing attacks, credential theft, and identity fraud.

Unknown Risk Profile:

Lack of transparency in security policies of cloud providers.

Enterprise-Wide Risk Management

- **A structured approach to identifying, assessing, and mitigating risks.**

- 6 Step process of Risk Administration is shown ->

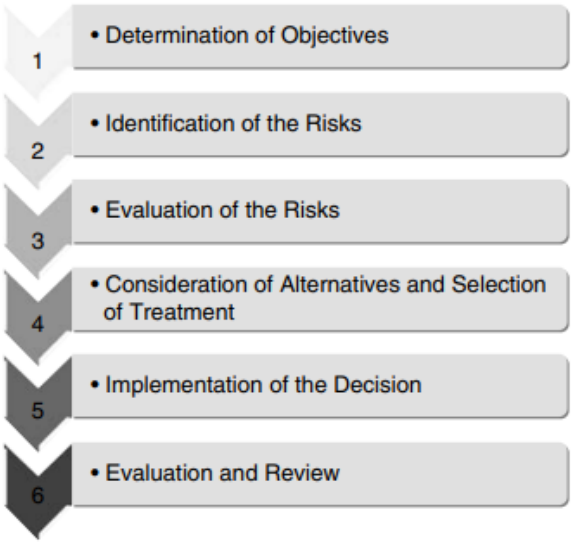

Figure 18.1 Six-step Risk Administration Process

6 Step process of Risk Administration

Step 1: Determining Objectives

- Maintain operational efficiency
- Protect employees from severe injury or loss

Step 2: Identifying Risks

- Awareness tools:
- Risk analysis questionnaires
- Exposure checklists

Step 3: Evaluating Risks

- Assess potential loss impact
- Determine likelihood of occurrence
- Categorize as:
  - ✓ Critical risks
  - ✓ Significant risks
  - ✓ Insignificant risks

6 Step process of Risk Administration

Step 4: Selecting Risk Management Strategies

- Analyze different approaches
- Choose appropriate mitigation method

Step 5: Risk Financing

- Risk retention vs. risk transfer
- Evaluate financial impact and available resources

Step 6: Evaluation & Review

- Continuously reassess risks
- Adapt to changing business environments

Security and Compliance Risks

Data Protection Risks:

- - Data residency laws requiring specific geographic storage.
- - Encryption challenges and unauthorized data access.

Regulatory Compliance:

- - Adhering to GDPR, HIPAA, ISO 27001, and other frameworks.
- - Maintaining audit trails and security certifications.

Disaster Recovery Challenges:

- - Need for proper backup strategies and failover mechanisms.
- - Risks of data loss due to cloud provider failures.

Service Downtime Risks:

- - Downtime affecting business operations and SLAs.
- - Evaluating redundancy measures and provider reliability.

Mitigation Strategies

Strong Access Controls

- - Multi-factor authentication (MFA) for user verification.
- - Role-based access control (RBAC) to limit privileges.

Data Encryption:

- - Secure encryption for data at rest and in transit.
- - Regular key rotation and robust key management policies.

Regular Audits:

- - Periodic security assessments and vulnerability scans.
- - Compliance audits for regulatory adherence.

Backup & Disaster Recovery Plans:

- - Ensuring offsite backups and quick data restoration processes.
- - Testing recovery plans to minimize downtime.

Vendor Evaluation:

- - Assessing service provider security measures and certifications.
- - Clear contract terms covering SLAs and data ownership.

Data Security in Cloud

- Cloud computing provides scalable and on-demand computing resources.
- Security is a major concern due to data storage in remote locations.
- Key security areas: data security, access control, compliance, and threat protection.

Parul®
University

DIGITAL LEARNING CONTENT

Digital Persona and Data Security

- Digital Persona: Online representation of a user's identity.
- Risks: Identity theft, impersonation, unauthorized access.
- Data security ensures confidentiality, integrity, and availability (CIA triad).

Content Level Security

- Protects specific types of content rather than the entire system.
- Techniques: Encryption, Digital Rights Management (DRM), Access Control Lists (ACLs).
- Ensures only authorized users can view or modify content.

Understanding the Shared Security Model

- Cloud security is a shared responsibility between the provider and the customer.
- Cloud Provider: Responsible for infrastructure security (hardware, network, virtualization).
- Customer: Responsible for securing applications, data, and access control.

Cloud Security Services

- Encryption services (e.g., AWS KMS, Azure Key Vault).
- Identity and access management (IAM).
- Security Information and Event Management (SIEM).
- Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS).

Authentication and Security Authorization

- Authentication: Verifies user identity (e.g., passwords, biometrics, MFA).
- Authorization: Grants or restricts access based on user roles and permissions.
- Examples: OAuth, Single Sign-On (SSO), Role-Based Access Control (RBAC).

Challenges in Cloud Security

- Data Breaches: Unauthorized access to sensitive data.
- Data Loss: Accidental deletion or corruption.
- Insider Threats: Employees or vendors misusing access.
- Regulatory Compliance: Meeting industry and legal security standards.

Software Testing in Cloud Security

- Penetration Testing: Simulated cyber-attacks to find vulnerabilities.
- Vulnerability Scanning: Automated checks for security weaknesses.
- Compliance Audits: Ensuring regulatory requirements are met.

Best Practices for Cloud Security

- Enable multi-factor authentication (MFA).
- Encrypt data at rest and in transit.
- Implement zero-trust security principles.
- Regularly monitor and audit access logs.

Parul®
University

DIGITAL LEARNING CONTENT

Future of Cloud Security

AI-driven threat detection.

- Zero-trust architecture.
- Blockchain for enhanced security.
- Quantum computing risks and solutions.

DIGITAL LEARNING CONTENT

Parul® University

www.paruluniversity.ac.in