



The Institute of Chartered Accountants of India

(Set up by an Act of Parliament)



Women & Young Members Excellence Committee

Organises

SkillUp Knowledge Webinar Series



CA. Purushottam H. Khandelwal
Chairman, WYMEC, ICAI



CA. Sripriya Kumar
Vice Chairperson, WYMEC, ICAI

Cloud Audit for Chartered Accountants

A Practical Approach to Auditing Cloud Environments

Session Speaker: CA Zalak Parikh, FCA, DISA, CISA, FAFD, Cloud Auditor, DPDPA Certified Partner U M Jintanwala & Co.

Organised by: Women and Young Members Committee of ICAI

Date: 15 July 2026

Why Should Chartered Accountants Understand Cloud?

- Accounting, payroll, ERP, email and customer data are increasingly hosted on cloud platforms.
- Even small entities rely extensively on Microsoft 365, Google Workspace, Zoho, Tally on Cloud and online backups.
- Traditional paper/physical evidence is disappearing; auditors must trace data trails residing completely online.
- Cloud infrastructure decisions directly affect internal financial controls, data protection, business continuity and statutory regulatory compliance.

OPENING QUESTION

"Where is your client's accounting and business data actually stored?"

As auditors, we cannot sign off on internal financial controls without verifying the security, location and integrity of the cloud hosting those records.

Cloud Industry Exposure in Actual Numbers

GLOBAL CLOUD PENETRATION

94% of enterprises globally use cloud services in some form today.

19.3% projected annual growth in worldwide public cloud spending.

\$1.42 Trillion expected global public cloud market size by 2029 (Gartner).

INDIA RAPID ADOPTION

\$17.5 Billion projected India public cloud spend in 2026 (up from \$13.7B in 2025).

28.1% annual cloud expenditure growth rate in India.

\$30.4 Billion expected Indian market by 2029, tracking 22.6% CAGR (IDC).

When an industry grows at over 20% annually, auditors cannot remain unfamiliar with its underlying systems and risks.

What Is Cloud Computing?

THE CONCEPT

Cloud computing is the delivery of on-demand computing services—including servers, storage, databases, networking, software, and analytics over the Internet ('the cloud') on a flexible, pay-as-you-go pricing model instead of maintaining physical local infrastructure.

EVERYDAY EXAMPLES IN BUSINESS

- ✓ Gmail & Google Drive
- ✓ Microsoft 365 (Office suites)
- ✓ Zoho Books & CRM
- ✓ Tally hosted on Cloud servers
- ✓ Online payroll, HR, and billing apps

THE POWER GRID ANALOGY

Traditional IT is like owning and running your own generator. You pay for the machine, maintenance, fuel, and staff regardless of how much electricity you actually consume.

Cloud Computing is like plugging into the national electrical grid. You consume power instantly, scale up or down freely, and pay only for the exact metered units you use.

Traditional IT Versus Cloud

Dimension	Traditional IT (On-Premises)	Cloud Environment
Location	Servers physically located in company office	Servers hosted in provider's secure remote data centers
Acquisition	Infrastructure purchased as capital assets (CapEx)	Infrastructure rented as operating expense subscription (OpEx)
Upfront Costs	High initial investment in hardware and licenses	No capital required; usage or monthly/annual plans
Scaling capacity	Slow manual upgrades required to expand	Instant scaling on-demand at the click of a button
Verification	Physical inspection of server room possible	Digital configurations, system settings, & reports reviewed
Control mapping	Company directly manages and secures all layers	Responsibility split dynamically between company and provider
Auditor Approach	Inspect physical assets, localized system logs	Review dashboard reports, SLAs, access controls, compliance docs

Audit Implication: Audit evidence shifts completely from physical inspection of server hardware to verifying electronic settings, contracts, access logs, and security reports.

Where Is Cloud Used in Business?

COMMON BUSINESS APPLICATIONS

- Accounting & Enterprise Resource Planning (ERP)
- Corporate Email, Messaging & Document Storage
- Payroll Management & HR Information Systems
- Customer Relationship Management (CRM)
- E-commerce, Websites & Customer Portals
- Banking & Instant Payment Gateway Integrations
- Automated Data Backups & Disaster Recovery systems
- Data Analytics, AI Modelling & Predictive Tools

CLOUD-NATIVE GIANTS

These globally and locally dominant brands have zero traditional server rooms. Their business platforms exist entirely in the cloud:

Global: Netflix, Zoom, Salesforce, Shopify, Airbnb

India: Swiggy, Zomato, Razorpay, Freshworks

Crucial Insight: *For these modern enterprises, the cloud is not a supportive IT utility. The cloud IS their business.*

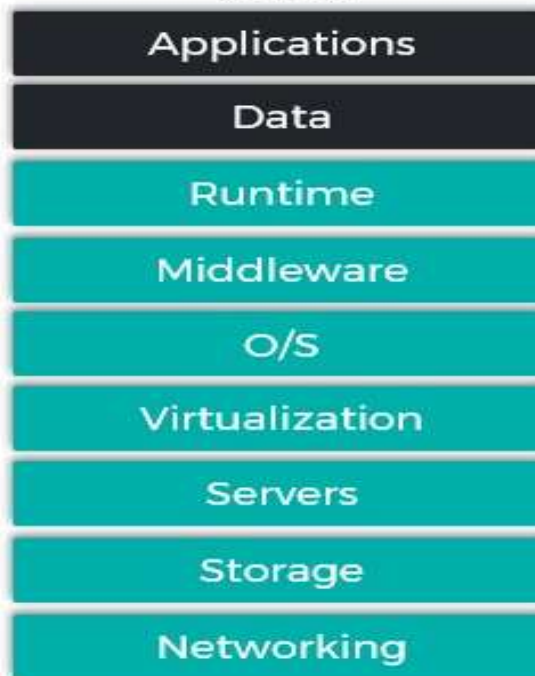
Three Types of Cloud Services

Infrastructure as a Service (IaaS)



 You Manage

Platform as a Service (PaaS)



 Provider Manages

Software as a Service (SaaS)



SaaS, PaaS and IaaS at a Glance

Model	What the Customer Receives	Simple Example	Customer Responsibility
SaaS	Ready-to-use software applications	Microsoft 365 / Zoho Books	Configuring system users, core data & basic security settings
PaaS	Managed platforms to deploy application code	Azure App Service / AWS Elastic Beanstalk	Developing the software application code, managing user databases
IaaS	Virtual server hardware, networks and storage	Amazon EC2 / Azure Virtual Machines	Installing Operating System, managing system firewall, full stack configuration

EASY MEMORY FORMULA: *SaaS: Use the Software | PaaS: Build on the Platform | IaaS: Manage the Infrastructure*

The customer's share of security and internal controls responsibility increases exponentially as you transition downward from SaaS to PaaS to IaaS.

Public, Private, Hybrid and Multi-Cloud

Public Cloud

Resources are owned and operated by third-party providers (e.g., AWS, Azure, Google Cloud). Multi-tenant infrastructure shared with other organisations, partitioned logically.

Private Cloud

Cloud infrastructure dedicated exclusively to a single organisation. Can be hosted on-site (own data center) or managed offsite by a specialized provider.

Hybrid Cloud

Ties on-premises traditional physical servers together with Public/Private cloud storage and applications, allowing secure data movement between both environments.

Multi-Cloud

Utilising cloud service pools from multiple public providers simultaneously to avoid vendor lock-in, balance costs, and secure geographic redundancy.

PRACTICAL MULTI-CLOUD HYBRID EXAMPLE: Client uses M365 (SaaS) for email, AWS (IaaS) for business website portal, Google Drive (SaaS) for document sharing, and local servers for legacy billing.

Who Is Responsible for Cloud Security?

THE PROVIDER RESPONSIBLE FOR: (Security OF the Cloud)

- 🔒 Physical security of building and data centers
- 🔒 Physical server maintenance, wiring, cooling
- 🔒 Core network cables, switches, routers
- 🔒 Hypervisor layer (the virtual machine manager)
- 🔒 Hardware life cycle and automated sanitization

THE CUSTOMER RESPONSIBLE FOR: (Security IN the Cloud)

- 🔑 User identities, authorization, password rules
- 🔑 Multifactor Authentication (MFA) settings
- 🔑 Data upload classification and security labels
- 🔑 Virtual network firewall configuration & open ports
- 🔑 Database security and backup frequencies

CRITICAL REAL-WORLD EXPOSURE EXAMPLE: AWS offers perfectly secure storage buckets. However, if the customer's administrator forgets to tick 'Block Public Access', the client's financial spreadsheets become viewable by anyone on the internet.

Gold Standard Rule: Outsourcing IT infrastructure does not mean outsourcing compliance or accountability.

What Is a Cloud Audit?

A CLOUD AUDIT EXAMINES WHETHER:

- The client maintains an accurate, updated cloud service inventory.
- Corporate ownership and review channels have been assigned.
- Admin rights are strictly limited and user directories pruned.
- Sensitive financial & personal information is securely encrypted.
- Comprehensive cloud logs are activated, secure, and monitored.
- Disaster recovery and backup restorations are regularly tested.
- Cloud vendor contracts (SLAs) guarantee data sovereignty.

IMPORTANT CLARIFICATION

A cloud audit is NOT just tech-heavy ethical hacking or penetration testing.

It is a thorough evaluation of Cloud Governance, administrative controls, user lifecycles, contractual vulnerabilities, data retention compliance, and operational resiliency.

Six Main Areas of Cloud Audit

1. Governance & Inventory

Do they maintain a golden list of approved SaaS, PaaS, and IaaS products? Are employees buying shadow IT applications on corporate credit cards without permission?

2. User Access & Admin

Is administrative privilege strictly controlled? Is Multifactor Authentication (MFA) forced on every dashboard? Are access rights instantly revoked for leavers?

3. Data Protection

Is critical client accounting and financial information encrypted at-rest inside the cloud storage buckets and in-transit across network tunnels?

4. Network Security

Are firewall rules configured to block untrusted external IP addresses? Are application portals shielded against modern internet DDoS threats?

5. Logging & Monitoring

Are operational dashboards tracking and storing every administrative action? Are automated alerts fired immediately if a storage bucket is made public?

6. Resiliency & Vendors

Are system backups isolated from main cloud accounts? Are cloud contracts reviewed for service availability, liability, and exit clauses?

Basic Audit Questions a CA Can Ask

Governance	Access	Data Security	Monitoring	Recovery
Q1. Which cloud services are being used across departments? Q2. Who is the designated owner of each platform? Q3. Do we have a central inventory updated monthly?	Q1. Who has administrator rights to these setups? Q2. Is Multi-Factor Authentication forced? Q3. Are former workers' accesses cut off immediately?	Q1. What classification of data resides on the cloud? Q2. Is sensitive financial data encrypted securely? Q3. Is any shared folder public by accident?	Q1. Are administrator activities logged properly? Q2. Who reviews security alerts and logs? Q3. Are system audit logs protected from alteration?	Q1. Is critical system and database data backed up? Q2. Are backup files kept offsite logically? Q3. Has data recovery actually been tested?

Practical Case Study: ABC Private Limited

CLIENT COMPOSITION & FINDINGS

 **Systems Utilised:** Microsoft 365, Tally on Cloud, Google Drive, AWS client portal, online payroll system.

Gap 1: No unified corporate inventory of cloud services exists.

Gap 2: Former payroll accountant still has access to Microsoft 365 panel.

Gap 3: Admin account MFA was disabled to 'save time' during billing runs.

Gap 4: Shared Google Drive folders contain sensitive banking PDFs set to 'Anyone with Link can Access'.

Gap 5: Backups exist, but database recovery drills were never conducted.

Gap 6: No contractual exit plan for transferring Tally data if the hosting vendor shuts down.

DISCUSSION POINTS FOR THE AUDIT TEAM

1. Which of these gaps represent critical Cloud Governance issues?
2. How does disabled administrator MFA threaten overall internal financial control integrity?
3. Which finding creates immediate public liability and regulatory penalty risks (DPDPA)?
4. What specific digital evidence should you collect to document these findings?

Aim of Case Study: *Demonstrate that auditing cloud setups does not require complex programming—it requires classic logical auditing instincts.*

Role of Chartered Accountants & Key Takeaways

HOW CAs DRIVE VALUE IN CLOUD AUDITING

- ✓ Evaluate Cloud Governance and vendor compliance frameworks
- ✓ Conduct enterprise-level logical risk assessments
- ✓ Verify user access lifecycles and administrative barriers
- ✓ Evaluate the operational depth of IT General Controls (ITGC)
- ✓ Perform critical vendor contract reviews (SLAs, penalties)
- ✓ Verify business continuity, backups and logical exit plans
- ✓ Map security configurations against regulatory baselines

FIVE KEY PRESENTATION TAKEAWAYS

1. Cloud infrastructure is now a standard baseline across businesses.
2. Cloud security is a shared responsibility, not completely outsourced.
3. SaaS, PaaS, and IaaS carry completely distinct risk configurations.
4. Administrator access levels, data leakage, and recovery drill statuses are optimal auditing starting points.
5. CAs are highly equipped to evaluate cloud governance and risk models, loop in technical specialists if complex configurations require deep deep-dive testing.

"The question is no longer whether our clients use the cloud. The real question is whether they understand and control the cloud they already use."