Course Title: Cloud Computing Auditing: Risks & Control Strategies

- **Duration:** 5 Days (approximately 35-40 instructional hours)
- **Course Goal:** To provide IT auditors, internal auditors, and risk/compliance professionals with the specialized knowledge, frameworks, and practical techniques required to effectively assess and audit the risks and controls associated with an organization's use of cloud computing services (IaaS, PaaS, SaaS), enabling them to provide meaningful assurance in a shared responsibility environment.
- **Core Focus:** Understanding the unique risks of the cloud, auditing the shared responsibility model, and leveraging provider attestations (like SOC reports) to perform effective cloud audits.

Learning Objectives:

Upon successful completion of this workshop, participants will be able to:

- **Define** cloud computing and differentiate between IaaS, PaaS, and SaaS service models.
- **Articulate** the Shared Responsibility Model and identify the specific control responsibilities of the cloud service provider (CSP) versus the cloud customer.
- **Identify** and assess key risks in a cloud environment, including data breaches, misconfigurations, compliance challenges, and vendor lock-in.
- **Apply** leading frameworks (e.g., CSA Cloud Controls Matrix, COSO) to scope and plan a cloud audit.
- **Design** audit procedures to test critical customer-managed controls in the cloud, particularly in Identity and Access Management (IAM).
- **Effectively** request, review, and interpret third-party assurance reports like SOC 1, SOC 2, and ISO 27001 certifications.
- **Audit** key cloud security domains, including data protection, network security, configuration management, and incident response.
- **Understand** the principles of cloud governance and cost management (FinOps).
- **Craft** clear and impactful audit findings and recommendations for cloud environments.
- **Develop** a comprehensive audit program for a specific cloud service (e.g., an IaaS or SaaS application).

Target Audience:

- IT Auditors and Senior IT Auditors.
- Internal Auditors responsible for auditing technology.
- Cybersecurity Professionals and Information Security Managers.
- Risk Management and Compliance Professionals.
- IT Leaders and Cloud Architects who want to understand the audit perspective.

Prerequisites:

- A strong understanding of fundamental IT audit principles and IT General Controls (ITGC).
- Familiarity with basic cybersecurity and networking concepts.
- Experience in conducting or managing IT audits is highly beneficial. (Certifications like CISA, CISSP are a plus).

Teaching Methodology:

This is a highly interactive, case-based, and technically-aware workshop. The methodology includes:

- **Interactive Lectures & Framework Deconstruction:** Breaking down cloud concepts and security frameworks into auditable components.
- **Case Study-Based:** A central case study of a fictional company migrating to and operating in the cloud will be used for all risk assessment and audit planning exercises.
- **Hands-on Workshops:** The core of the course. Participants will work in teams to define shared responsibilities, analyze SOC reports, and develop audit test steps.
- **Technical Evidence Review:** Analyzing sample technical evidence like IAM policies, network security group rules, and cloud configuration reports.

ADEPT TRAINING CENTER

- **Tabletop Exercises:** Simulating scenarios like responding to a cloud security incident or a data breach.
- **Group Discussions & Peer Learning:** A collaborative environment for sharing audit approaches and challenges in the cloud.

*(For **Online Delivery**, this will be adapted using virtual whiteboards (e.g., Miro/Mural) for mapping responsibilities, breakout rooms for case study work, collaborative documents for audit program development, and screen sharing for evidence review.)*

Materials Provided:

- Comprehensive digital or printed workbook with key cloud concepts, risk frameworks, audit methodologies, and best practices.
- An "Cloud Auditor's Toolkit" with templates for a Shared Responsibility Matrix, a SOC Report Review Checklist, and a Cloud Audit Program.
- A detailed case study with supporting documents (e.g., cloud architecture diagrams, sample security policies, an excerpt from a SOC 2 report).
- Publicly available copies of the CSA Cloud Controls Matrix (CCM).
- Certificate of Completion.

Detailed Day-by-Day Curriculum

Day 1: The Cloud Audit Universe – Concepts & Risks

- **Module 1: Introduction to Cloud Computing for Auditors (Approx. 2.5 hours)**
  - Welcome, introductions, and course objectives.
  - Defining Cloud Computing (NIST definition).
  - Deep dive into the Service Models: **IaaS** (Infrastructure), **PaaS** (Platform), **SaaS** (Software).
  - Deployment Models: Public, Private, Hybrid, Multi-cloud.
  - Key benefits and fundamental shifts from on-premise IT.
  - **Activity:** "Classify the Service" – Participants categorize various technology services (e.g., Salesforce, AWS EC2, Dropbox) into IaaS, PaaS, or SaaS.
- **Module 2: The Shared Responsibility Model: The Core of Cloud Auditing (Approx. 2.5 hours)**
  - Understanding the fundamental principle: The CSP is responsible for the security *of* the cloud; the customer is responsible for security *in* the cloud.
  - Mapping responsibilities for IaaS, PaaS, and SaaS across different control domains (e.g., physical security, network controls, OS patching, data encryption).
  - Why this model changes everything for auditors.
  - **Workshop:** Participants work in groups to fill out a Shared Responsibility Matrix for the case study's use of a specific cloud service.
- **Module 3: The Cloud Risk Landscape (Approx. 2.5 hours)**
  - Identifying unique and amplified risks in the cloud:
    - **Misconfigurations:** The #1 cause of cloud breaches.
    - **Identity & Access Management (IAM) Complexity.**
    - **Data Breaches & Data Loss.**
    - **Lack of Visibility & "Shadow IT."**
    - **Compliance & Data Sovereignty Issues.**
    - **Vendor Lock-in & Concentration Risk.**
  - **End of Day 1 Recap & Q&A.**

Day 2: Auditing Cloud Governance & The Power of Third-Party Assurance

- **Module 4: Auditing Cloud Governance & Strategy (Approx. 2.5 hours)**
  - Assessing the organization's cloud strategy and adoption policy.
  - Auditing the Cloud Center of Excellence (CCoE) or governance function.

ADEPT TRAINING CENTER

- Reviewing cloud security policies and standards.
- The importance of a cloud data classification policy.
- Introduction to Cloud FinOps (Financial Operations) and auditing cost management.

- **Module 5: Leveraging Third-Party Assurance: SOC Reports (Approx. 3 hours)**
  - How auditors gain assurance over the CSP's controls.
  - Differentiating between **SOC 1**, **SOC 2**, and **SOC 3** reports.
  - Deep dive into a **SOC 2 Report:**
    - Type 1 vs. Type 2.
    - Understanding the Trust Services Criteria (Security, Availability, Processing Integrity, Confidentiality, Privacy).
    - Key sections to review: Auditor's Opinion, Management's Assertion, System Description, Control Testing.
  - The critical importance of reviewing User Control Considerations (UCCs).
- **Module 6: Analyzing SOC 2 Reports & Other Attestations (Approx. 2 hours)**
  - **Hands-on Workshop:** Participants are given an excerpt of a real (anonymized) SOC 2 report.
  - They work in groups to:

1. Identify the audit opinion.
2. Understand the scope of the report.
3. Analyze a set of control tests and results.
4. Identify key User Control Considerations that their organization must implement.

  - Brief overview of other key attestations: ISO 27001, CSA STAR.
  - **End of Day 2 Recap & Q&A.**

Day 3: Auditing the Customer's Responsibility – Identity & Infrastructure

- **Module 7: The Most Critical Domain: Auditing Identity & Access Management (IAM) (Approx. 3.5 hours)**
  - Why IAM is the new security perimeter in the cloud.
  - Key IAM concepts: Users, Groups, Roles, Policies.
  - Audit procedures for assessing:
    - **Root Account Security** (MFA, no access keys).
    - The principle of **Least Privilege**.
    - Password policies and Multi-Factor Authentication (MFA) enforcement.
    - User access review processes for the cloud.
    - Use of roles vs. individual user permissions.
    - Key management and encryption key access.
  - **Evidence Review Workshop:** Analyzing sample IAM policies (in JSON or human-readable format) to identify weaknesses.
- **Module 8: Auditing IaaS Infrastructure Security (Approx. 2.5 hours)**
  - Auditing customer responsibilities for IaaS (e.g., AWS EC2, Azure VMs).
  - **Network Security:** Auditing Virtual Private Clouds (VPCs), subnets, and network security groups (firewall rules).
  - **Compute Security:** Auditing OS patching, vulnerability management, and endpoint protection on virtual machines.
- **Module 9: Auditing Configuration Management & "Infrastructure as Code" (IaC) (Approx. 1.5 hours)**
  - The risk of manual misconfigurations.
  - Auditing the use of IaC (e.g., Terraform, CloudFormation) for consistent and secure deployments.
  - Reviewing Cloud Security Posture Management (CSPM) tool reports.

ADEPT TRAINING CENTER

- **End of Day 3 Recap & Q&A.**

Day 4: Auditing Data Protection, Operations & SaaS

- **Module 10: Auditing Data Protection in the Cloud (Approx. 3 hours)**
  - Auditing data classification implementation.
  - **Encryption:** Auditing encryption of data at rest (e.g., on storage volumes) and data in transit (using TLS).
  - Auditing backup and disaster recovery processes for customer-managed data.
  - Reviewing Data Loss Prevention (DLP) controls in the cloud.
- **Module 11: Auditing Logging, Monitoring & Incident Response in the Cloud (Approx. 2.5 hours)**
  - Assessing the configuration of cloud logging services (e.g., AWS CloudTrail, Azure Monitor).
  - Auditing the process for monitoring logs and generating alerts (integration with SIEM).
  - Evaluating the cloud-specific Incident Response plan.
  - **Tabletop Exercise:** A facilitated walkthrough of a security incident in a cloud environment.
- **Module 12: Auditing SaaS Applications (Approx. 2 hours)**
  - Shifting the audit focus for SaaS (e.g., Microsoft 365, Salesforce).
  - Key audit areas for SaaS:
    - **Vendor Due Diligence & SOC Report Review.**
    - **User Access Controls & Permissions** within the application.
    - **Application Configuration Security.**
    - **Data Integration & API Security.**
    - **Data Export & Exit Strategy.**
  - **Workshop:** Developing a high-level audit plan for a new, critical SaaS application.
  - **End of Day 4 Recap & Q&A.**

Day 5: Reporting, The Future & Your Cloud Audit Plan

- **Module 13: Crafting Impactful Cloud Audit Reports (Approx. 2.5 hours)**
  - The challenge of communicating cloud risks and shared responsibilities.
  - Writing clear, concise findings that differentiate between CSP and customer responsibilities.
  - Developing actionable recommendations for customer-managed controls.
  - Using risk ratings and visualizations to communicate posture to the Audit Committee.
- **Module 14: Continuous Cloud Auditing & The Future of Cloud Assurance (Approx. 2 hours)**
  - Moving from periodic audits to continuous assurance.
  - The role of Cloud Security Posture Management (CSPM) and other automated tools in continuous monitoring.
  - Auditing serverless and containerized environments (overview of risks).
  - The evolving skillset of the cloud auditor.
- **Module 15: Capstone: Developing a Cloud Audit Program (Approx. 2.5 hours)**
  - **Capstone Workshop:** Participants work in groups to develop a comprehensive audit program for the case study organization's primary cloud environment (e.g., their AWS IaaS deployment).
  - The program will include:
    1. Audit Objectives and Scope.
    2. Key Risks and Control Objectives (based on CSA CCM or NIST CSF).
    3. High-level audit procedures for key areas like IAM, Network Security, and Data Protection.
    4. Evidence to be requested.
  - Groups present their audit programs for peer and instructor feedback.

ADEPT TRAINING CENTER

- **Module 16: Course Review & Your Action Plan (Approx. 1 hour)**
    - Review of the key frameworks and methodologies for auditing the cloud.
    - Open forum for final questions.
    - **Action Planning:** Participants identify key steps they can take to build cloud audit capabilities in their organization.
    - Course evaluation and closing.

ADEPT TRAINING CENTER