Cloud Computing
for CPAs

Course Description

The Coronavirus (COVID-19) crisis led to a global lockdown that changed how we live and work. The contagion of COVID-19 created an increased need for remote work. Companies of all sizes are adopting cloud-based solutions and embracing online productivity and collaboration services. Cloud migration is a business platform strategy with many deciding factors. Thus, before making cloud computing an integral part of the technology infrastructure, one should recognize the potential benefits and risks.

This course is divided into three parts. Part I addresses concepts of cloud computing in simple terms, its features, and types of deployment. It covers the benefits of cloud computing as well as the most relevant legal issues involved in cloud environments. Part II discusses how each service model satisfies a unique set of business requirements and explores the advantages and disadvantages of each model. It also includes recommendations for mitigating the risks of these models. Part III explains cloud security risks, threats, and vulnerabilities. It also identifies security standards and frameworks to help both providers and customers, providing security baselines, validations, and certifications.

Completion Deadline & Exam: This course, including the examination, must be completed within one year of the date of purchase.

Course Level: Overview. This program is appropriate for professionals at all organizational levels.
CPE Credits: 3 (CPA)
Category: Information Technology
Prerequisite: None
Advanced Preparation: None

Course Learning Objectives

Cloud Computing

After studying this course you will be able to:

1. Identify the different types of cloud deployment models, including their features and use cases

2. Recognize legal considerations (e.g., data privacy, data flow restrictions) for cloud computing
3. Identify major cloud service models and their benefits and limitations
4. Recognize the shared responsibility model that dictates the obligations of a provider and its customers
5. Recognize the risks and vulnerabilities in cloud environments
6. Identify major cloud security standards, frameworks, and certifications