# CTS2375C Cloud Infrastructure and Services

## Course Description:
This course helps students develop technical expertise in cloud computing and prepares them for the AWS (Amazon Web Services) Solutions Architect - Associate certification exam. Students will learn the essentials of cloud computing, business security and compliance considerations, migrating to the cloud, architecting a cloud server, and how to troubleshoot cloud services. (3 hr. lecture 2 hr. lab)

## Course Competency

### Competency 1:
The student will demonstrate an understanding of the business essentials required to implement and support a cloud network by:

1. Explaining the value and benefits of the AWS Cloud. Discussing the security capabilities, controls, and assurances in place to maintain security and data protection. Identifying the financial impact the AWS cloud can have on an organization’s procurement cycle, cost management, and contracts. Discussing best practices for the successful implementation and operation of an IT environment with AWS components.

### Competency 2:
The student will demonstrate an understanding of the technical essentials of the AWS Cloud by:

1. Describing an Amazon Virtual Private Cloud (VPC). Navigating the AWS Management Console. Identifying the security measures AWS provides. Describing the AWS Storage option. Using Amazon Elastic Compute Cloud (EC2) and Amazon Elastic Block Storage (EBS) to create an Amazon Simple Storage Service (S3) bucket and manage associated objects. Identifying the different AWS compute and networking options. Describing Managed Services and Database options, including: describing Amazon DynamoDB, verifying key aspects of Amazon RDS, executing an Amazon RDS drive application. Launching an application using Amazon Relational Database Service (RDS). Identifying deployment and management options, including: identifying AWS CloudFormation, describing Amazon CloudWatch metrics and alarms, describing Amazon Identity and Access Management (IAM).

### Competency 3:
The student will demonstrate how to plan and design the AWS architecture by:

1. Identifying cloud architecture considerations (e.g., fundamental components, effective designs, etc.), including: designing cloud services, monitoring cloud services, best practices in designing and incorporating cloud services, developing to Client Specifications including pricing/cost (e.g., on Demand vs. Reserved vs. Spot, RTO and RPO DR Design), architectural trade-off decisions (high availability vs. cost, using AWS Managed Services vs. Doing It Yourself (DIY), integrating with existing development environments and building scalable architecture, elasticity and scalability. Making architectural decisions based on AWS recommended architectural principles and best practices, including: designing storage services, leveraging global infrastructure, choosing a data store, designing web-scale media hosting, orchestrating batch processing, reviewing large-scale design
patterns, designing for cost, planning for distributed environments. Designing event-driven scalable, highly available, and fault tolerant servers. Incorporating security best practices into cloud design. Creating a cloud migration roadmap and plan, including extending on-premises into the cloud. Creating business continuity and disaster recovery plans.

**Competency 4:** The student will demonstrate how implement and deploy AWS by:

1. Identifying the appropriate techniques and methods to code and implement a cloud solution (i.e., Amazon EC2, Amazon S3, Elastic Beanstalk, CloudFormation, Amazon Virtual Private Cloud (VPC), AWS Identity and Access Management (IAM). Configuring an Amazon Machine Image (AMI). Operating and extending service management in the private cloud. Configuring compliance in the private and public cloud. Launching instances in a variety of geographical regions. Lifting and shifting existing on-premises applications to AWS. Ingressing and egressing of data to and from AWS Selecting the appropriate AWS service based on data, compute, database, or security requirements. Identifying appropriate use of AWS architectural best practices Estimating AWS costs and identifying cost control mechanisms. Troubleshooting and monitoring performance.

**Competency 5:** The student will demonstrate an understanding of cybersecurity procedures for optimum cloud deployment and maintenance by:

1. Discussing cloud security best practices. Applying AWS Security Architecture services, including: AWS Shared Security Responsibility Model, AWS Platform Compliance, AWS security attributes (e.g., customer workloads down to the physical layer), Security Services, AWS Identity and Access Management (IAM), Amazon Virtual Private Cloud (VPC), CIA and AAA models, ingress vs. egress filtering, and which AWS services and features fit, “Core” Amazon EC2 and S3 security feature sets, Amazon CloudWatch. Developing a threat model. Creating a data flow diagram for risk management to include use cases and abuse/negative use cases. Incorporating common conventional security products (Firewall, IDS/HIDS/NIDS, SIEM, VPN). Creating design patterns. Mitigating Distributed Denial-of-Service (DDoS) attacks encryption solutions. Implementing complex access controls (e.g., building sophisticated security groups, ACLs, etc.).

**Competency 6:** The student will demonstrate an understanding of disaster recovery techniques by:

1. Discussing disaster recovery issues and considerations. Differentiating between “pilot light” and “hot standby” environments. Identifying how to apply AWS disaster recovery (DR) architectures (e.g., pilot light, hot standby, etc.). Designing a disaster recovery plan. Describing how to apply the elements of Amazon Elastic Block Store (EBS) to a disaster recovery architecture, including: AWS Import/Export, AWS Storage Gateway, Amazon Route53. Testing the recovered data.