Module 1 – Introduction to Cloud Security

# \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Overview and Objectives

## Overview

In this module, we will introduce the definition of cloud computing provided by the National Institute of Standards and Technology (NIST) and discuss its essential characteristics, service models, and deployment models. Then we will discuss how cloud computing introduces new security challenges, but also offers new opportunities to achieve better security.

**COURSE LEVEL OBJECTIVES (CLO)**

**Upon completion of this course, you should be able to:**

1. Recognize and identify terminology and concepts related to Cloud Computing.
2. Compare and contrast technology that enables and supports the effective and secure use of Cloud Computing infrastructures.
3. Explore an array of security and privacy issues in Cloud Computing systems, current best practices, and open problems to provide recommendations that add value to an organization’s Cloud-based products or services.
4. Be able to identify, research, and recommend best practices related to legal and regulatory issues pertaining to Cloud Computing.
5. Discuss and evaluate Cloud Computing and security related issues.

## Module level Objectives (MLO)

**Upon completion of this module’s activities, you should be able to:**

1. Recognize and identify terminology and concepts related to the definition of Cloud Computing. (CLO 1)
2. Compare and contrast Cloud Computing and traditional IT. (CLO 1, 2)
3. Classify cloud instances based on their service and deployment models. (CLO 1, 2)
4. Identify and compare key security challenges and benefits of Cloud Computing. (CLO 2, 3)

# \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Module Video (Wiley-Produced w/Dan Ramos) [3-5 minutes]

* Script

# \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Learning Materials [~100 pages, ~10 hours]

## Textbook Readings

* Chee, B., & Franklin Jr., C. (2019). Securing the Cloud: Security Strategies for the Ubiquitous Data Center (1st ed.). Auerbach Publications.
  + Chapter 1, 2

## Other Readings

* NIST Special Publication 800-145
* “An Overview of Cloud Computing” from The Next Wave, Vol 17, No 4, 2009
* A FedRAMP Overview: Introduction, <https://youtu.be/I_3YFkmGTt4>

# \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Module 1 Learning Unit 1 – Introduction to Cloud Computing (MLO 1, 2, 3,4) [~3 hours]

* **1. Glossary entries**
  + **Tenants** typically lease a dynamically provisioned piece of the cloud infrastructure in the form of either IaaS or PaaS to provide services to their users.
  + **End users** typically interact with or consume specific application services that are deployed in a cloud.
  + A cloud is **internal** when it is on the organization’s premises. It is **external** when it is physically located in a third party’s facility.
  + A cloud is **insourced** when it is operated by the organization’s own staff. It is **outsourced** when it is operated by a third party.
* **2. Self-assessment activity**. Before diving into the course, and without consulting any books or other references, write a short description of what you think cloud computing is. At the end of the course, you will be asked to re-examine your original definition in light of what you learned from the course.
* **3. Learning Element**: Cloud Computing Milestones [Note: this could be turned into an interactive timeline]
  + In 2008, the idea that an enterprise would entrust its data and operations to a computing platform on which functionality was decoupled from specific hardware or geography was completely new and was at the cutting edge of enterprise information technology.
    - Amazon Web Services was launched in 2006
    - Google App Engine was released in 2008
    - Microsoft announced its Azure Services Platform in October 2008
    - IBM Cloud was released in 2011
  + ***Reading***: “An Overview of Cloud Computing” from The Next Wave, Vol 17, No 4, 2009 (skip section on MapReduce)
* **4. Screencast**: Definition of Cloud Computing [M1-LU1-Screencast-1 - Definition of Cloud Computing]
  + ***Reading***: NIST Special Publication 800-145
* **7. Learning element**: Other important cloud characteristics
  + NIST-defined characteristics are important, but not binding: *“The NIST definition … is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion … The service and deployment models defined form a simple taxonomy that* ***is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation****.”* – NIST SP800-145
  + Another key characteristic of cloud computing is the service interface between the provider and the consumer, which is defined by a Service Level Agreement (SLA): *"It is represented by a contract that enforces the value proposition with guarantees (SLA) and terms (price). Everything that happens to make clouds stand out as something new is due to this interface. It enables competition, drives the cost behavior of the seller, and the value choices of the buyer. Without it, you just have enterprise IT at work.”* – Bill Meine
  + Reliable network connectivity is also critical for the operation of any cloud deployment: without reliable network connectivity, consumers will not be able to access their data and applications when needed.
* **6.Interactive activity**: Cloud Dimensions [M1-LU1-Activity – Cloud Dimensions.pptx]
* **7. Learning element**: Opportunities and Concerns
  + Cloud Computing is an evolutionary outgrowth of prior computing approaches, from mainframes to grid computing. It builds upon existing technologies but offers new opportunities around the notion of shared computing resources.
  + Cloud Computing is not inherently more or less secure than traditional IT.
  + **Opportunities**
    - Cloud Computing is revolutionizing and democratizing access to Information Technology in the same way the Internet has revolutionized and democratized access to information.
      * This computing paradigm is ideal for startups, which would not otherwise be able to invest in their own IT infrastructure.
    - The economies of scale that the cloud model promises to deliver are enticing. Vendors can minimize their operating costs and pass some of the savings on to the consumers
  + **Concerns**
    - **Erosion of control**. The loss of control due to decoupling functionalities from hardware and geography represents a concern for many organizations. Organizations with stringent security requirements may not be willing to give up control to cloud providers.
    - **Concerns about cloud storage**
      * The risk that, in a multi-tenancy model, failing isolation mechanisms might expose data to unauthorized parties
      * The possibility that a cloud provider might store data in multiple jurisdictions
      * The fact that storage might be implemented in a single centralized location, thus creating a single point of failure
      * Secondary use of the data collected by cloud providers, that is unauthorized use for a purpose other than the one for which the data was originally collected.
      * The viability of cloud providers.
      * Compliance of providers with data privacy laws and regulations.
    - **Concerns about applications**
      * Major public cloud providers impose their own architectures and application program interfaces (APIs), thus making it difficult for consumers to migrate to a different provider, a phenomenon known as cloud lock-in.
  + The adoption of cloud computing is increasing, but security concerns still represent the major factor stopping some organizations from moving to cloud. Unfortunately, cloud computing is evolving so rapidly that regulations and security technology have not necessarily been able to keep pace.
* **6. Learning element**: Protection of the Cloud and by the Cloud
  + **Protection of the Cloud**: a Cloud Computing deployment is an IT infrastructure and, like any IT infrastructure, needs to be secured.
  + **Protection by the Cloud**: cloud-based security services can help secure traditional IT (Security-as-a-Service).

# \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Module 1 Learning Unit 2 – A New Model for Security (MLO 1, 2, 4) [~3 hours]

* **1. Glossary entries**
  + **FISMA** is the **Federal Information Security Management Act of 2002**, which recognized the importance of information security to the economic and national security interests of the United States**.**
  + The **Federal Risk and Authorization Management Program (FedRAMP)** is a United States federal government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Video: A FedRAMP Overview: Introduction (<https://youtu.be/I_3YFkmGTt4>).
  + The **Payment Card Industry Data Security Standard (PCI DSS)** is an information security standard for organizations that handle credit cards from the major payment networks.
* **2. Learning element**: Evolution of Security
  + Cloud security is an extension of recognized and established security principles into cloud-based deployments. These principles can be applied to (1) protect the cloud, (2) protect traditional IT infrastructure from the cloud, or (3) a hybrid of the two.
  + Three key qualities of successful cloud implementations are massive scale, a disciplined appearance, and repeated patterns. By developing suitable repeated patterns and implementing them on a massive scale, cost savings can be achieved during all phases of the cloud life cycle. These same qualities also have a significant role with respect to security, as implementing security at scale is more cost-effective.
  + Interesting quotes about cloud scale:
    - *“Upon entering a data center that hosts a cloud infrastructure, you will notice the immense size of the space and the overwhelming noise that comes from countless identically racked computers that are all neatly cabled and look the same”* -- Vic Winkler, Securing the Cloud, 2011.
    - *“This is the sound of lots of data being crunched and lots of data being stored... All around you, the other end of these machines, there may be tens of thousands or millions of people doing what they need to do. They have no idea that these things are here. This is the Internet. We’re sitting in the Internet. We’re surrounded by it. It's breathing in the wall behind us.”* – Dan Butzer, Sun Microsystems, NPR 2009.
* **3. Learning element**: Regulations, policies, and procedures
  + Securing IT infrastructure is not merely a technical problem, and it involves administrative aspects. In fact, access controls can be classified as administrative, technical, and physical.
    - **Administrative access controls** are the procedures defined by an organization to implement and enforce overall access control (e.g., hiring practices, background checks, security training). Depending on the industry, some of these controls may be required by law.
    - **Technical access controls** are the hardware or software mechanisms used to manage access to resources and systems (e.g., firewalls, intrusion detection systems, access control lists).
    - **Physical access controls** are physical barriers deployed to prevent direct contact with systems or areas within a facility (e.g., gates, mantraps, guards).
  + Cloud computing is evolving so rapidly that regulations and security technology have not necessarily been able to keep up. This means that IT professionals are frequently left to adapt pre-existing regulations, models, and technologies to new infrastructures and architectures for which they may be poor fits.
  + Both government and industry have established rules and standards for protecting IT infrastructure, including cloud.
    - The Federal Information Security Management Act of 2002 (FISMA) lays out rules, developed by the National Institute for Science and Technology (NIST) for protecting information, but does not prevent agencies from storing data or using applications in the cloud. A government “cloud first” policy actually encouraged agencies to use cloud services to reduce costs.
    - To help both government agencies adopting cloud services and cloud vendors providing services to government agencies, the federal government established the Federal Risk and Authorization Management Program (FedRAMP), a government-wide program that provides a standardized approach to security assessment, authorization, and monitoring cloud products and services.
* **4. Screencast**: Shared Responsibility over Security [M1-LU2-Screencast-1 - Shared responsibility]
* **5. Interactive activity**: Control over Security [M1-LU2-Activity - Control over Security.pptx]
* **6. Learning element**: Location-Independent Security
  + Moving data and applications to the cloud creates a sense of location independence. Users and tenants can access cloud-based resources from anywhere through a variety of thin and thick clients, and those same resources may be scattered across multiple geographic locations if the cloud vendor manages multiple datacenters across different regions.
  + The same level of security must be guaranteed independently of where data and applications are physically located and of where users and tenants are accessing them from. However, identity management must be location-aware, by relying on hardware or software that uses any of several techniques to determine its geographic location.
    - *Consider the following scenario*. A user swipes their card to get physical access to a computing facility and connects to one of their company’s cloud-based applications via VPN from a foreign country. When considered in isolation, both events may be perfectly legitimate. However, if they happen at approximately the same time, a location-aware identity and access management system should recognize that the user couldn’t possibly have been in two different places at the same time, so this event could be a security breach.
  + A prime example of the application of location-aware computing principles is geotargeting for Internet marketing, which uses knowledge of the user’s physical location to deliver targeted advertisements. In general, the idea is that, while access to services and the mechanics to secure it should be independent of the user’s location, the system’s behavior can adapt based on knowledge of the user’s location.
* **7. Learning element**: Layered Security or Defense-in-Depth

# \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Module 1 Assignment 1 – Comparing Cloud Computing and Traditional IT (MLO 1, 2) [~2 hours]

**Purpose**

The purpose of this assignment is to have students think critically about how Cloud Computing can eliminate the typical inefficiencies of traditional server closets or data centers.

**Instructions**

Traditional *server closets* or *data centers* may be highly inefficient when compared to a cloud solution. Identify the key inefficiencies and discuss how migrating to a cloud solution would address such inefficiencies.

**Deliverable**

Submit a short essay in Word or PDF format, 2 pages maximum (e.g., 11pt, single-spaced, times new roman, 1-inch margins) with your response to the instructions for the case.

**Due Date**

Your assignment is due by Sunday 11:59 PM, ET.

# \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Module 1 Quiz (MLO 1, 2, 3,4) [~.5 hour]

**Purpose**

Quizzes in this course give you an opportunity to demonstrate your knowledge of the subject material.

**Instructions**

Note the following instructions for your quiz:

* The quiz is 20 minutes in length.
* The quiz is closed-book.

**Deliverable**

Use the link above to take the quiz.

**Due Date**

Your quiz submission is due by Sunday 11:59 PM, ET.

# \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_