Course Outline:

This course is broken out into 6modules that cover the 13 domains of the CSA Guidance and the ENISA Cloud Computing: Benefits, Risks and Recommendations for Information Security.

M**odule 1**: Introduction to Cloud Computing. This module covers the fundamentals of cloud computing, including definitions, architectures, and the role of virtualization. Key topics include cloud computing service models, delivery models, and fundamental characteristics. It also introduces a model for assessing the risk of moving to the cloud.

Module 2: Infrastructure Security for Cloud Computing. This modules digs into the details of securing the core infrastructure for cloud computing- including cloud components, networks, management interfaces, and administrator credentials. Students will learn the key components to public and private clouds and techniques for securing them.

Module 3: Managing Cloud Security and Risk. This module covers important considerations for managing security for cloud computing. It begins with risk assessment and governance, then covers legal and compliance issues, such as discovery requirements in the cloud. It finishes with a discussion or portability and interoperability and managing incident response when working with cloud providers.

Module 4: Data Security for Cloud Computing. One of the biggest issues in cloud security is protecting data. This module covers information lifecycle management for the cloud and how to apply security controls, with an emphasis on public cloud. Topics include the Data Security Lifecycle, cloud storage models, data security issues with different delivery models, and managing encryption in and for the cloud.

Module 5: Application Security and Identity Management for Cloud Computing. This module covers identity management and application security for cloud deployments. Topics include federated identity and different IAM applications, secure development, and managing application security in and for the cloud.

Module 6: Selecting Cloud Services. This module covers key considerations when evaluating, selecting, and managing cloud computing providers. It includes important questions to ask and what to look for. We also discuss the role of Security as a Service providers.

Second Day (please bring your own laptop):

This second day of training includes additional lecture, although student's will spend most of their time assessing, building, and securing a cloud infrastructure during the exercises.

Exercise 1: Introduction and Risk Analysis. Students will be introduced to the day's scenario and build a threat model for migrating to the cloud.

Exercise 2: Create and Secure a Public Cloud Instance. Students will create a basic cloud instance on a public cloud infrastructure and establish a security baseline. Topics include creating an AWS instance, establishing network security, and understanding machine images.

Exercise 3: Encrypt Public Cloud Data. In this module students will dive into cloud storage options and learn the basics to encrypt data for their public cloud deployment.

Exercise 4: Create and Secure a Cloud Application: Now the students will secure their first public application for the cloud, following best practices such as architecting their cloud application stack and managing appropriate network security.

Exercise 5: Identity Management for the Cloud. Students will create a basic federated identity infrastructure to support their cloud application and learn additional details on standards like SAML and OAuth.