Overview
Students will learn the basic Cloud types and delivery models and develop an understanding of the risk and compliance responsibilities and challenges for each Cloud type and service delivery model. The student will also learn how to apply RSA’s trust-based security model to real-world security problems. The course concludes with a module on guidance for building private Clouds and a lab exercise where the student will implement a private cloud using a 3rd party provider’s interface.

Some materials in this course have been developed in conjunction with the Cloud Security Alliance. A Certificate of Cloud Computing Security Knowledge (CCSK) is available through the Cloud Security Alliance.

Audience
This course is intended for RSA/EMC customers who have virtualized a portion of their environment and wish to acquire Cloud services either externally via a public Cloud or to implement Cloud technologies internally (private Cloud). This course will be valuable for those who work in security or virtualization administration, compliance, architecture, and audit roles within their organization.

Duration
4 days

Prerequisite Knowledge/Skills
- Basic familiarity with IT concepts, including storage, computation and networking
- Working knowledge of TCP/IP networking technologies (equivalent to CompTIA Network+ certification)
- Working knowledge of Information Security concepts (equivalent to CompTIA’s Security+ certification)
- Conversant with virtualization concepts
- Comfortable using a command-line interface

Course Objectives
Upon successful completion of this course, participants should be able to:
- Identify security aspects of each cloud model
- Develop a risk-management strategy for moving to the Cloud
- Implement a public cloud instance using a public cloud service provider
- Apply RSA’s trust-based security model to different layers in the infrastructure stack
- Distinguish between cloud providers and 3rd party managed service providers
Course Outline

- Introduction to Cloud Computing
  - Cloud Overview
  - Cloud Service Models
  - Cloud Deployment Models

- Managing Cloud Security and Risk
  - Impact of Cloud Tiers on Security and Risk
  - Standards Organization
  - RSA's Cloud Trust model
  - Things to Look for in a Cloud Provider

- Infrastructure Layer Trust
  - Infrastructure Trust Layer Definition
  - Disaster Recovery
  - Virtualization
  - Segmentation and Isolation
  - Log Management
  - Secure Communications
  - Multi-Tenancy

- Application Layer Trust
  - Application Layer Trust: definition
  - Web Application Security Fundamentals
  - Application Security Phases and Lifecycle
  - SDLC
  - PaaS Security Concerns

- Information Layer Trust
  - Information Layer Trust: Definition
  - Data Retention / Destruction
  - Data Leakage
  - Data Privacy
  - Data Encryption and Key Management
  - Data Geolocation
  - E-Discovery
  - Data Portability
  - Data Classification

- Management
  - Management Layer Trust: Definition
  - Identity and Access Management
  - Roles and Responsibilities
  - Provider Viability
  - Compliance Monitoring
  - Business Continuance
  - Provider Supply Chain
  - Third-party Risk Assessment
  - Software Licensing Risk

- Securing Private Clouds
  - Enterprise IT Evolution
  - Private Cloud Security Primer

- Final Lab Exercise
  - Hands-on exercise in which participants are challenged to build a best-in-class vendor data application with minimal assistance