QUALITY THOUGHT
#208 B, Nilgiri Block, Aditya Enclave, Ameerpet

Cloud Security

Mode of Training: Online, Corporate

Course Duration:40 Hours

Course Curriculum

Domain 1 Introduction to IT Security

The goal of this domain is to provide you with a brief introduction to some basic security concepts that are integral to all security professionals and will help you understand the cloud security concepts with ease. This will also help aspirants who are new to the IT security world. Below are the concepts covered in this domain:

- Least Privilege
- Defense in Depth
- Confidentiality, Integrity, Availability
- Cryptography
- Certificates
- Physical Security
- Risk Management
- Business Continuity and Disaster Management

    - Basic Security Concepts
    - Risk Management
    - Business Continuity and Disaster Recovery

Domain 2 Architectural Concepts and Design Requirements

The goal of the Architectural Concepts and Design Requirements domain is to provide you with knowledge of the building blocks necessary to develop cloud-based systems. You will be introduced to cloud computing concepts regarding topics such as the customer, provider, partner, measured services, scalability, virtualization, storage, and networking. You will also be able to understand the cloud reference architecture based on activities defined by industry-standard documents. Lastly, you will gain knowledge in relevant security and design principles for cloud computing, including secure data lifecycle and cost-benefit analysis of cloud-based systems. Platform and the data handling aspects of the platform

- Cloud Computing Concepts
- Cloud Reference Architecture
- Security Concepts Relevant to Cloud Computing
- Design Principles of Secure Cloud Computing
- Identifying Trusted Cloud Services
- Cloud Architecture Models

    - Cloud Computing Concepts
        - Cloud Computing Definitions
        - Cloud Computing Roles
        - Key Cloud Computing Characteristics
        - Building-Block Technologies
    - Cloud Reference Architecture
        - Cloud Computing Activities
        - Cloud Service Capabilities
        - Cloud Service Categories
        - Cloud Deployment Models

    - Cloud Cross-Cutting Aspects

- ✓ Security Concepts Relevant to Cloud Computing
    - Cryptography
    - Access Control
    - Data and Media Sanitation
    - Network Security
    - Virtualization Security
    - Common Threats
    - Security Considerations for the Different Cloud Categories
- ✓ Design Principles of Secure Cloud Computing
    - Cloud Secure Data Lifecycle
    - Cloud-Based Business Continuity/Disaster Recovery Planning
    - Cost–Benefit Analysis
- ✓ Identify Trusted Cloud Services
    - Certification Against Criteria
    - System/Subsystem Product Certifications
    - ISO/IEC 27001 and 27001:2013
    - NIST SP 800-53
    - Payment Card Industry Data Security Standard (PCI DSS)
    - SOC 1, SOC 2, and SOC 3
    - Common Criteria
    - FIPS 140-2
- ✓ Cloud Architecture Models
    - Sherwood Applied Business Security Architecture (SABSA)
    - IT Infrastructure Library (ITIL)
    - The Open Group Architecture Framework (TOGAF)
    - NIST Cloud Technology Roadmap

Domain 3 Cloud Data Security

The goal of the Cloud Data Security domain is to provide you with knowledge of the types of controls necessary to administer various levels of confidentiality, integrity, and availability, regarding securing data in the cloud. You will gain knowledge on topics of data discovery and classification techniques; digital rights management; privacy of data; data retention, deletion, and archiving; data event logging, chain of custody and non-repudiation; and the strategic use of security information and event management.

- ➢ Understanding the Cloud Data Lifecycle
- ➢ Design and Implement Cloud Data Storage Architectures
- ➢ Design and Apply Data Security Strategies
- ➢ Data Discovery and Classification Techniques
- ➢ Relevant Jurisdictional Data Protections for PII
- ➢ Data Rights Management
- ➢ Data Retention, Deletion and Archiving Policies
- ➢ Auditability, Traceability and Accountability of Data Events

- ✓ Understanding the Cloud Data Lifecycle
  - Phases
- ✓ Design and Implement Cloud Data Storage Architectures
  - Storage Types
  - Threats to Storage Types
  - Technologies Available to Address Threats
- ✓ Design and Apply Data Security Strategies
  - Encryption
  - Key Management
  - Masking/Obfuscation / Anonymization
  - Tokenization
  - Application of Technologies
  - Emerging Technologies
- ✓ Data Discovery and Classification Techniques
  - Data Discovery
  - Classification
- ✓ Relevant Jurisdictional Data Protections for Personally Identifiable Information
  - Data Privacy Acts
  - Privacy Roles and Responsibilities
  - Implementation of Data Discovery
  - Classification of Discovered Sensitive Data
  - Mapping and Definition of Controls
  - Application of Defined Controls
- ✓ Data Rights Management
  - Data Rights Objectives
  - Tools
- ✓ Data Retention, Deletion, and Archiving Policies
  - Data Retention
  - Data Deletion
  - Data Archiving
- ✓ Auditability, Traceability, and Accountability of Data Events
  - Definition of Event Sources
  - Identity Attribution Requirements
  - Data Event Logging
  - Storage and Analysis of Data Events
  - Continuous Optimizations
  - Chain of Custody and Nonrepudiation

Domain 4 **Cloud Platform and Infrastructure Security**

The goal of the Cloud Platform and Infrastructure Security domain is to provide you with knowledge regarding both the physical and virtual components of the cloud infrastructure. You will gain knowledge regarding risk-management analysis, including tools and techniques necessary for maintaining a secure cloud infrastructure. In addition to risk analysis, you will gain an understanding of how to prepare and maintain business continuity and disaster recovery plans, including techniques and concepts for identifying critical systems and lost data recovery. Stepping stones to the cloud

- ➢ Cloud Infrastructure Components
- ➢ Risks Associated with Cloud Infrastructure
- ➢ Design and Plan Security Controls
- ➢ Disaster Recovery and Business Continuity Management Planning

  - ✓ Cloud Infrastructure Components
    - Physical Environment
    - Networking
    - Computing
    - Virtualization
    - Storage
    - Management Plane
  - ✓ Risks Associated with Cloud Infrastructure
    - Risk Assessment and Analysis
    - Virtualization Risks
    - Countermeasure Strategies
  - ✓ Design and Plan Security Controls
    - Physical and Environmental Protection
    - System and Communication Protection
    - Virtualization Systems Protection
    - Management of Identification, Authentication, and Authorization
    - Auditing
  - ✓ Disaster Recovery and Business Continuity Management Planning
    - Understanding the Cloud Environment
    - Understanding Business Requirements
    - Understanding Risks
    - Disaster Recovery/Business Continuity Strategy

Domain 5 **Cloud Application Security**

The goal of the Cloud Application Security domain is to provide you with knowledge as it relates to cloud application security. Through an exploration of the software development lifecycle, you will gain an understanding in utilizing secure software and understand the controls necessary for developing secure cloud environments and program interfaces. You will gain knowledge in identity and access management solutions for the cloud and the cloud application architecture. You'll also learn how to ensure data and application integrity, confidentiality, and availability through cloud software assurance and validation.

- ➢ Training and Awareness in Application Security
- ➢ Cloud Software Assurance and Validation
- ➢ Verified Secure Software
- ➢ Understanding the Software Development Lifecycle Process
- ➢ Applying the Secure Software Development Lifecycle
- ➢ Cloud Application Architecture
- ➢ Identity and Access Management Solutions

- ✓ Training and Awareness in Application Security
    - Cloud Development Basics
    - Common Pitfalls
    - Common Vulnerabilities
- ✓ Cloud Software Assurance and Validation
    - Cloud-Based Functional Testing
    - Cloud Secure Development Lifecycle
    - Security Testing
- ✓ Verified Secure Software
    - Approved API
    - Supply-Chain Management
    - Community Knowledge
- ✓ Understanding the Software Development Lifecycle (SDLC) Process
    - Phases and Methodologies
    - Business Requirements
    - Software Configuration Management and Versioning
- ✓ Applying the Secure Software Development Lifecycle
    - Cloud-Specific Risks
    - Quality of Service
    - Threat Modeling
- ✓ Cloud Application Architecture
    - Supplemental Security Devices
    - Cryptography
    - Sandboxing
    - Application Virtualization
- ✓ Identity and Access Management (IAM) Solutions
    - Federated Identity
    - Identity Providers
    - Single Sign-On
    - Multifactor Authentication

Domain 6 Operations

The goal of the Operations domain is to explain the requirements needed to develop, plan, implement, run, and manage the physical and logical cloud infrastructure. You will gain an understanding of the necessary controls and resources, best practices in monitoring and auditing, and the importance of risk assessment in both the physical and logical cloud infrastructures. With an understanding of specific industry compliance and regulations, you will know how to protect resources, restrict access, and apply appropriate controls in the cloud environment.

- ➢ Support the Planning Process of Data Center Design
- ➢ Implement and Build the Physical Infrastructure for Cloud Environment
- ➢ Run and Manage the Physical Infrastructure for Cloud Environment
- ➢ Build the Logical Infrastructure for Cloud Environment
- ➢ Run and Manage the Logical Infrastructure for Cloud Environment

- Ensure Compliance with Regulations and Controls
- Conduct Risk Assessment for Physical and Logical Infrastructure
- Understanding of Collection, Acquisition, and Preservation of Digital Evidence
- Manage Communication with Relevant Parties

- ✓ Support the Planning Process for the Data Center Design
  - Logical Design
  - Physical Design
  - Environmental Design
- ✓ Implement and Build the Physical Infrastructure for the Cloud Environment
  - Secure Configuration of Hardware-Specific Requirements
  - Installation and Configuration of Virtualization Management Tools
- ✓ Run the Physical Infrastructure for the Cloud Environment
  - Configuration of Access Control for Local Access
  - Securing Network Configuration
  - OS Hardening via the Application of Baselines
  - Availability of Standalone Hosts
  - Availability of Clustered Hosts
- ✓ Manage the Physical Infrastructure for the Cloud Environment
  - Configuring Access Controls for Remote Access
  - OS Baseline Compliance Monitoring and Remediation
  - Patch Management
  - Performance Monitoring
  - Hardware Monitoring
  - Backup and Restore of Host Configuration
  - Implementation of Network Security Controls
  - Log Capture and Analysis
  - Management Plan
- ✓ Build the Logical Infrastructure for the Cloud Environment
  - Secure Configuration of Virtual Hardware–Specific Requirements
  - Installation of Guest Operating System Virtualization Toolsets
  - un the Logical Infrastructure for the Cloud Environment
  - Secure Network Configuration
  - OS Hardening via Application of Baselines
  - Availability of the Guest Operating System
- ✓ Manage the Logical Infrastructure for the Cloud Environment
  - Access Control for Remote Access
  - OS Baseline Compliance Monitoring and Remediation
  - Patch Management
  - Performance Monitoring
  - Backup and Restore of Guest OS Configuration
  - Implementation of Network Security Controls
  - Log Capture and Analysis
  - Management Plan

- ✓ Ensure Compliance with Regulations and Controls
  - Change Management
  - Continuity Management
  - Information Security Management
  - Continual Service Improvement Management
  - Incident Management
  - Problem Management
  - Release and Deployment Management
  - Configuration Management
  - Service Level Management
  - Availability Management
  - Capacity Management
- ✓ Conduct Risk Assessment for the Logical and Physical Infrastructure
  - Framing Risk
  - Assessing Risk
  - Responding to Risk
  - Monitoring Risk
- ✓ Understand the Collection, Acquisition, and Preservation of Digital Evidence
  - Proper Methodologies for the Forensic Collection of Data
  - Evidence Management
- ✓ Manage Communication with Relevant Parties
  - Vendors
  - Customers
  - Partners
  - Regulators
  - Other Stakeholders

Domain 7 **Legal and Compliance Domain**

The goal of the Legal and Compliance domain is to provide you with an understanding of how to approach the various legal and regulatory challenges unique to cloud environments. To achieve and maintain compliance it is important to understand the audit processes utilized within a cloud environment, including auditing controls, assurance issues, and the specific reporting attributes. You will gain an understanding of ethical behaviour and required compliance within regulatory frameworks, which includes investigative techniques for crime analysis and evidence-gathering methods. Enterprise risk considerations and the impact of outsourcing for design and hosting are also explored.

- ➢ Legal Requirements and Unique Risks within Cloud Environment
- ➢ Privacy Issues and Jurisdictional Variation
- ➢ Audit Processes, Methodologies and Required Adaptations for Cloud Environment
- ➢ Implications of Cloud to Enterprise Risk Management
- ➢ Outsourcing and Cloud Contract Design
- ➢ Executive Vendor Management

- ✓ Legal Requirements and Unique Risks Within the Cloud Environment
  - International Legislation Conflicts
  - Appraisal of Legal Risks Specific to Cloud Computing
  - Legal Controls
  - eDiscovery
  - Forensics Requirements
- ✓ Privacy Issues and Jurisdictional Variation
  - Difference Between Contractual and Regulated PII
  - Country-Specific Legislation Related to PII and Data Privacy
  - Differences Among Confidentiality, Integrity, Availability, and Privacy
- ✓ Audit Processes, Methodologies, and Required Adaptions for a Cloud Environment
  - Internal and External Audit Controls
  - Impact of Requirements Programs by the Use of Cloud
  - Assurance Challenges of Virtualization and Cloud
  - Types of Audit Reports
  - Restrictions of Audit Scope Statements
  - Gap Analysis
  - Audit Plan
  - Standards Requirements
  - Internal Information Security Management System (ISMS)
  - Internal Information Security Controls System
  - Policies
  - Identification and Involvement of Relevant Stakeholders
  - Specialized Compliance Requirements for Highly Regulated Industries
  - Impact of Distributed IT Model
- ✓ Implications of Cloud to Enterprise Risk Management
  - Assess Providers Risk Management
  - Difference Between Data Owner/Controller vs. Data Custodian/Processor
  - Risk Mitigation
  - Different Risk Frameworks
  - Metrics for Risk Management
  - Assessment of the Risk Environment
- ✓ Outsourcing and Cloud Contract Design
  - Business Requirements
  - Vendor Management
  - Contract Management
- ✓ Executive Vendor Management
  - Supply-Chain Management

Last Mile: **Project Work**

The goal of project work is to help you get a hold of applying cloud security concepts and principles that you learned throughout this course to real-time scenario. This will be a hands- on exercise which covers real-time scenario.

- ➢ Project work covering real-time scenarios

Supporting Enterprises around the Globe

Established in 2010

Quality Thought®

The Leader in Software Training

www.qualitythought.in

☎ 040- 40025423

✉ info@qualitythought.in