CCSO - Certified Cloud Security Officer

Course Overview

This course will teach students about Cloud Security. Topics covered include cloud risks, legal implications, data center operations, incident response, application security, and more.

Chapter 1 - Introduction to Cloud Computing and Architectural Concepts 2h 2m

Course Introduction
Introduction to Cloud Computing and Architectural Concepts
Where are we?
What are we covering?
Section 1: Cloud Computing Terminology
Key Cloud Computing Terminology
Key Cloud Computing Terminology
Terminology Mapped to the Cloud
Other Terms
Section 2: Cloud Computing Definition
Cloud Computing Defined
NIST Five Essential Characteristics
NIST Three Service Models
SaaS Pros and Cons
PaaS Pros and Cons
IaaS Pros and Cons
NIST Four Deployment Models
Cloud Computing Characteristics
Section 3: Cloud Computing Benefits
Why move to the Cloud?
Cost Benefit Analysis
Cost Benefit Analysis
Cost Benefit Analysis
ROI Calculation
TCO Calculation
Ease of Deployment – Security Risks
Introductory Security Risks and Benefits
Section 4: Cloud Computing Reference Model
Cloud Computing Architecture
Potential Pitfalls and Confusion
Cloud Computing Deployment Models
Jericho Cloud Cube Model
Example of Service Model Mapped to Controls
Section 5: What is Security for the Cloud
The Security Impact of Cloud Architecture
Where is the security added?
Cloud Technology Road Map

Chapter 3 - ERM and Governance 48m

ERM and Governance

What are we covering?

Section 1: Application of Governance and Risk Management to the Cloud

Corporate Governance

Corporate Governance

Customer Expectations

Four Areas Impacted

Tools of the Trade

Who is responsible? Not Accountable!

Cloud Computing Governance Resources

Information/Data Governance Types

Enterprise Risk Management

Risk Response in the Cloud

Where do we start?

Must do items

Section 2: Importance of the SLA

Contracts/SLAs

Contracts/SLAs: Change Your Thinking

Important SLA Components

Metrics for Risk Management/Service Level Agreement (SLA)

Section 3: CCM Relevant Controls

GRM-01 – Baseline Requirements

GRM-02 – Data Focus Risk Assessments

GRM-03 – Management Oversight

GRM-04 – Management Program

GRM-05 – Management Support/Involvement

GRM-06 – Policy

GRM-07 – Policy Enforcement

GRM-08 – Policy Impact on Risk Assessments

GRM-09 – Policy Reviews

GRM-10 – Risk Assessments

GRM-11 – Risk Management Framework

Questions

Chapter 4 - Legal Implications 59m

Legal Implications

Course Outline

What are we covering?

Section 1: Understanding Unique Risks in the Cloud

Understand Legal Requirements & Unique Risks Within the Cloud Environment

Section 2: International Legislation and Potential Conflicts

International Legislation Conflicts

International Legislation Conflicts

GDPR

International Legislation Conflicts

International Legislation Conflicts

Appraisal of Legal Risks Specific to Cloud Computing

Legal Controls

Section 3: eDiscovery

eDiscovery
Special Issues
Special Issues
eDiscovery
Forensics Requirements
Section 4: Contract Considerations
Contract Considerations
Contractual & Regulated PII: The Differences
Contractual & Regulated PII: The Differences
Contractual & Regulated PII: The Similarities
Country-specific Legislation Related to PII/Data Privacy/Data Protection
Section 5: Relevant CCM Controls
SEF-01 – Contract / Authority Maintenance
Questions

Chapter 5 - Virtualization and Technical Design 1h 42m

Virtualization and Technical Design
Course Outline
What are we covering?
Section 1: Virtualization Principles
Virtualization Definition
How Does Virtualization Work?
What is a Virtual Machine (VM)?
What is a Hypervisor?
Type 1 and Type 2 Hypervisors
Virtualization Layer
CPU Hardware Virtualization
Section 2: Key Components Mapped to Cloud Layer
vSphere 6.x Virtual Switches
VMware vSwitch Terminology
Storage Terminology
Overview of Virtual Appliances
Clones and Templates
Customization Specifications Manager
vSphere Content Libraries
VM Snapshots
vMotion – Hot Migration
Storage vMotion
Distributed Resource Scheduler Overview
Distributed Power Management (DPM)
VM Swapfile Location
Host Profiles Overview
Storage DRS (SDRS) Overview
Profile Driven Storage Overview
VSAN Architecture
Resource Pools Overview
High Availability Overview
Fault Tolerance
Section 3: Key Security Concerns
Virtualization Risks and Challenges

Network Security and Perimeter
Virtualization Security
Common Architecture Concerns
vSphere Hardening Guide
Section 4: Other Technologies Used in the Cloud
Network Security
Network and Communications in the Cloud
Cloud Networking - VXLAN
Section 5: The Layers
Logical Design Considerations
Physical, Virtual and vCloud Layers
Software-Defined Data Center (SDDC) - Components
SDDC – Physical Configuration
SDDC – vCenter Cluster Layout
SDDC – The Big Ugly Picture
SDDC – The Big Ugly Picture but not as bad!
Section 6: Relevant CCM Controls
IVS-01 – Audit Logging / Intrusion Detection
IVS-02 – Change Detection
IVS-03 – Clock Synchronization
IVS-04 – Information System Documentation
IVS-05 – Vulnerability Management
IVS-06 – Network Security
IVS-07 – OS Hardening and Base Controls
IVS-08 – Production / Non-Production Environments
IVS-09 – Segmentation
IVS-10 – VM Security – Data Protection
IVS-11 – Hypervisor Hardening
IVS-12 – Wireless Security
IVS-13 – Network Architecture
Questions

Chapter 6 - Managing Information and Securing Data 1h 53m

Managing Information and Securing Data
Course Outline
What are we covering?
Section 1: Cloud/Data Life Cycle
Data Security Lifecycle
Locations and Access
Functions, Actors, and Controls
Section 2: Data Security Architectures and Strategies
Pillars of Functionality
Storage Types IaaS
Storage Types PaaS
Storage Types SaaS
Top Threats to Storage
Technologies available to address the threats
Data Dispersion
Data Loss Prevention (DLP)
Data Loss Prevention (DLP)

DSI-01 – Management Classification
DSI-02 – Data Inventory Flows
DSI-03 – eCommerce Transactions
DSI-04 – Handling / Labeling / Security Policy
DSI-05 – Non-Production Data
DSI-06 – Ownership / Stewardship
DSI-07 – Secure Disposal
Questions

Chapter 7 - Data Center Operations 59m

Data Center Operations
Course Outline
What are we covering?
Section 1: The Logical Infastructure
Logical Infastructure Design Notes
Secure Configuration of Hardware Requirements
Secure Network Configuration
Hardening OS and Apps
Availability of Guest OS
Managing the Logical Infrastructure
IT Service Management (ITSM)
Information Security Management
Configuration Management Process
Configuration, Change and Availability Management
Shadow IT
Change Management Objectives
Change Management Policies and Procedures
Problem Management
Release and Deployment Management Objectives
Release and Deployment Management
Service Level Management
Other Management areas
Section 2: Manage Communications with all Parties
5 Ws and the H
Vendors
Customers
Partners
Section 3: Relevant CCM Controls
CCC-01 – New Development / Acquisition
CCC-02 – Outsourced Development
CCC-03 – Quality Testing
CCC-04 – Unauthorized Software Installations
CCC-05 – Production Changes
HRS-01 – Asset Returns
HRS-02 – Background Screening
HRS-03 – Employment Agreements
HRS-04 – Employment Terminations
HRS-05 – Mobile Device Management
HRS-06 – Non-Disclosure Agreements
HRS-07 – Roles / Responsibilities

HRS-08 – Technology Acceptable Use
HRS-09 – Training Awareness
HRS-10 – User Responsibility
HRS-11 – Workspace
STA-01 – Data Quality and Integrity
STA-02 – Incident Reporting
STA-03 – Network / Infrastructure Services
STA-04 – Provider Internal Assessments
STA-05 – Supply Chain Agreements
STA-06 – Supply Chain Governance Reviews
STA-07 – Supply Chain Metrics
STA-08 – Third Party Assessment
STA-09 – Third Party Audits
Questions

Chapter 8 - Interoperability and Portability 45m

Interoperability and Portability
Course Outline
What are we covering?
Section 1: Interoperability
Interoperability
Reason a change may happen
Why is this important
Example
Recommendations
Recommendations
Recommendations
Section 2: Portability
Portability
Interoperability and Portability Helps to Mitigate
Golden Rule
Basic Recommendations
Basic Recommendations
IaaS Recommendations
IaaS Recommendations
IaaS Recommendations
PaaS Recommendations
PaaS Recommendations
SaaS Recommendations
SaaS Recommendations
Private Cloud Recommendations
Public Cloud Recommendations
Hybrid Cloud Recommendations
Section 3: Relevant CCM Controls
IPY-01 – API's
IPY-02 – Data Request
IPY-03 – Policy and Legal
IPY-04 – Standardized Network Protocols
IPY-05 – Virtualization
Questions

Chapter 9 - Traditional Security 56m

Traditional Security
Course Outline
What are we covering?
Section 1: The Physical Environment
Physical Environment
Physically. What does one of these beasts look like?
Major Factors in building a great datacenter
Google’s Top 10
Datacenter Design
Network and Communications in the Cloud
Compute
Storage
Physical and Environmental Controls
Protecting Datacenter Facilities
System and Communication Protections
Section 2: Planning Process for the Data Center Design
Support the Planning
Physical Design Considerations
DC Design Standards
Tier Standard Review
Tiered Model Summary
Environmental Design
Environmental Design
Design Considerations
Multi-Vendor Pathway Connectivity (MVPC)
Section 3: Implement and Build Physical Infrastructure
Enterprise Operations
Security Requirements for Hardware
Oversubscription
iSCSI Implementation Considerations
Section 4: Typical Security for the Datacenter Components
Access Controls
Access Control (KVM)
Access Controls
Securing Network Configurations
OS Hardening
Everything about the OS
Stand-alone Host Availability Considerations
Availability of Clustered Hosts
Clustered Storage Architectures
Performance Monitoring
Redundant System Architecture
Backup and Restore of Hosts?
Log Management Recommendations
Log Management
Management Planning Includes
Business Continuity & Disaster Recovery
Business Continuity Elements
Section 5: Relevant CCM Controls

DCS-01 – Asset Management
DCS-02 – Controlled Access Points
DCS-03 – Equipment Identification
DCS-04 – Off-Site Authorization
DCS-05 – Off-Site Equipment
DCS-06 – Policy
DCS-07 – Secure Area Authorization
DCS-08 – Unauthorized Persons Entry
DCS-09 – User Access
Questions

Chapter 10 - BCM and DR 34m

BCM and DR
Course Outline
What are we covering?
Section 1: Disaster Recovery and Business Continuity Management
The Business Continuity Management Concept
BCM Lifecycle
Business Continuity Disaster Recovery
BCDR Relevant Cloud Characteristics
Business Impact Analysis
BCDR Requirements
BCDR Risks Requiring Protection
BCDR Strategy Risks
BCDR Strategies
Creating the BCDR Plan
Planning, Testing and Review
Section 2: Examples
Virtualization Pass Through
Backup and DR Software
Section 3: Relevant CCM Controls
BCR-01 – Business Continuity Planning
BCR-02 – Business Continuity Testing
BCR-03 – Datacenter / Utilities Environmental Conditions
BCR-04 – Operational Resilience Documentation
BCR-05 – Environmental Risks
BCR-06 – Equipment Location
BCR-07 – Equipment Maintenance
BCR-08 – Equipment Power Failures
BCR-09 – Impact Analysis
BCR-10 – Policy
BCR-11 – Retention Policy
Questions

Chapter 11 - Incident Response 37m

Incident Response
Course Outline
What are we covering?
Section 1: Incident Management
Incident Management

Incident Management Plan
Incident Classification
Security Events
Logs
Alerts
What is an Incident?
Security Incident
Indication of Compromise
What is Incident Handling?
Difference between IH and IR
Difference between IH and IR
Difference between IH and IR
Common Tools
IPS vs WAF
SOC
Six Step Approach to Incident Handling
Section 2: Forensics
Cloud Forensics Challenges
Methodology for Forensics
Access to Data by Service Model
Forensic Readiness Considerations
Items to consider when collecting evidence
Section 3: Relevant CCM Controls
SEF-01 – Contract / Authority Maintenance
SEF-02 – Incident Management
SEF-03 – Incident Reporting
SEF-04 – Legal Preparation
SEF-05 – Incident Response Metrics
Questions

Chapter 12 - Application Security 1h 21m

Application Security
Course Outline
What are we covering?
Section 1: Components affecting Security
Web Application Security
Application Basics
Application Programming Interface (API)
WS-* Features Web Services
Common Pitfalls
Encryption Dependencies
Section 2: Software Development Life Cycle (SDLC)
Software Development Lifecycle (SDLC)
Secure Software Development Lifecycle
S-SDLC
Software Development Lifecycle
Project Initiation
Requirements Phase
Requirements Phase
Secure Design

Chapter 13 - Encryption and Key Management 18m

Encryption and Key Management
Course Outline
What are we covering?
Section 1: Review from other chapters
You are the teacher now!
Cryptography
Encryption / Data Protection
Encryption & Key Management
Emerging Technologies
Section 2: Key Management in today's cloud services
Key Management Interoperability Protocol (KMIP)
KMIP
Vendors offering KMIP
Vendors that support KMIP
Cloud Access Security Broker (CASB)
Hardware Security Module (HSM)
Section 3: Recommendations
General Recommendations
Recommendations – Encryption with Databases
Section 4: Relevant CCM Controls
EKM-01 – Entitlement
EKM-02 – Key Generation
EKM-03 – Sensitive Data Protection
EKM-04 – Storage and Access
Questions

Chapter 14 - Identity, Entitlement and Access Management 46m

Identity, Entitlement and Access Management
Course Outline
What are we covering?
Section 1: Introduction to Identity and Access Management
Terms Used
Terms Used
Identity and Access Management
Identity, Entitlement, & Access Management
Key points to consider
Identity Architecture Differences
Identity Architecture Differences
Generic Example
Identity Federation
General Usage of Federation
Section 2: Identities and Attributes
Provisioning
Examples of Identities and Attributes
Potential Decision Making Process
Identity and the Attribute
Entitlement Process
Automated Approaches
Interpretation Locations

Authorization and Access Management
Section 3: Options for Architectures
Hub and Spoke Model
Mesh or Free Form Model
Free Form Model
Hybrid Model
Bridge or Federation Hub
Provisioning Accounts
Identity and Attribute Provisioning
Section 4: The Identity
Identity and Data Protection
Consumerization Challenge
Section 6: Relevant CCM Controls
IAM-01 – Audit Tools Access
IAM-02 – Credential Lifecycle / Provision Management
IAM-02 – Continued
IAM-02 – Continued
IAM-03 – Diagnostic /Configuration Port Access
IAM-04 – Policies and Procedures
IAM-05 – Segregation of Duties
IAM-06 – Source Code Access Restriction
IAM-07 – Third Party Access
IAM-08 – Trusted Sources
IAM-09 – User Access Authorization
IAM-10 – User Access Reviews
IAM-11 – User Access Revocation
IAM-12 – User ID-Credentials
IAM-13 – Utility Programs Access
Questions

Chapter 15 - Auditing and Compliance 54m

Auditing and Compliance
Course Outline
What are we covering?
Section 1: Compliance and Audit Cloud Issues
GRC Value Ecosystem
Assurance by CSP
Assurance by CSP – Assurance Frameworks
Assurance Challenges of Virtualization and Cloud
Assurance Challenges of Virtualization and Cloud
Assurance Challenges of Virtualization and Cloud
Assurance Challenges of Virtualization and Cloud
Policies
Policies
Risk Audit Mechanisms
Section 2: Assurance Frameworks
Assurance by CSP – Assurance Frameworks
Certification Against Criteria
Assurance Frameworks – ISO 2700X
ISO/IEC 27001 Domains

Assurance Frameworks – AICPA SOC 1
SOC II and SOC III
Assurance Frameworks – NIST SP 800-53
PCI-DSS Merchant Level
PCI-DSS 12 Requirements
PCI-DSS 12 Requirements
Assurance Frameworks – COBIT
Assurance Frameworks – AICPA/CICA Trust Services
Assurance Frameworks – Cloud Security Matrix
Assurance Frameworks – FedRamp
NIST SP 800-144
NIST SP 800-144 – Preliminary Activities
NIST SP 800-144 – Initiating & Coincident Activities
NIST SP 800-144 – Concluding Activities
Assurance Frameworks – HITRUST
Assurance Frameworks – BITS
Assurance Frameworks – Jericho SAS
System/Subsystem Product Certification
Common Criteria Protection Profiles (PP)
Section 3: The Audit
Cloud Audit Goals
Impact of Requirements Programs by the Use of Cloud
Types of Audit Reports
Types of Audit Reports
Restrictions of Audit Scope
Gap Analysis
Standards Requirements (ISO/IEC 27018, GAPP)
Internal ISMS
Internal Information Security Control System ISO 27002:2013
Cloud Computing Audit Characteristics
Internal and External Audit Controls
Internal and External Audit Controls
Planning & Scoping the Audit
Planning & Scoping the Audit
Planning & Scoping the Audit
Planning & Scoping the Audit
Planning & Scoping the Audit
Section 4: Relevant CCM Controls
AAC-01 – Audit Planning
AAC-02 – Independent Audits
AAC-03 – Information System Regulatory Mapping
Questions

Total Duration: 15h 50m