**C838 Studyplan and Keywords**

**Week 1**

Introduction

**Domain 1: Architectural Concepts and Design Requirements**

**WGU Competency: Secure Cloud Data Solutions**

Lesson 1: Architectural Concepts

Lesson 2: Design Requirements

Lesson 13: Domain 1: Architectural Concepts and Design Requirements

**Week 2**

**Domain 2: Cloud Data Security**

**WGU Competency: Secure Cloud Infrastructure**

Lesson 3: Data Classification

Lesson 4: Cloud Data Security

Lesson 14: Domain 2: Cloud Data Security

**Week 3**

**Domain 3: Cloud Platform and Infrastructure Security**

**WGU Competency: Critical Cloud Requirements**

Lesson 5: Security in the Cloud

Lesson 6: Responsibilities in the Cloud

Lesson 15: Domain 3: Cloud Platform and Infrastructure Security

**Week 4**

**Domain 4: Cloud Application Security**

**WGU Competency: Cloud Software Assessment**

Lesson 7: Cloud Application Security

Lesson 16: Domain 4: Cloud Application Security

**Week 5**

**Domain 5: Operations**

**WGU Competency: Manage Cloud Operations**

Lesson 8: Operations Elements

Lesson 9: Operations Management

Lesson 17: Domain 5: Operations

**Week 6**

**Domain 6: Legal and Compliance**

**WGU Competency: Legal and Compliance Cloud Requirements**

Lesson 10: Legal and Compliance Part 1

Lesson 11: Legal and Compliance Part 2

Lesson 18: Domain 6: Legal and Compliance

**Week 7**

**WGU Competency: Secure Cloud Data Solutions**

**WGU Competency: Secure Cloud Infrastructure**

**WGU Competency: Critical Cloud Requirements**

**WGU Competency: Cloud Software Assessment**

**WGU Competency: Manage Cloud Operations**

**WGU Competency: Legal and Compliance Cloud Requirements**

Lesson 12: Security Guidance

Review

**Week 8**

Objective Assessment

**Domains**:

**Domain 1 – Architectural Concepts and Design Requirements.**

**Domain 2 –** **Cloud Data Security.**

**Domain 3 – Cloud Platform Infrastructure Security.**

**Domain 4 – Cloud Application Security.**

**Domain 5 – Operations.**

**Domain 6 – Legal and Compliance.**

**Domain 1 Architectural Concepts and Design Requirements.**

NIST 800-145

NIST 800-146

Functional requirements

Nonfunctional requirements

Existing State

Quantifying Benefits and Opportunity Cost

Reduction in Capital Expenditure

Reduction in Personnel Costs

Reduction in Operational Costs

Transferring Some Regulatory Costs

Elasticity

Simplicity

Scalability

Cloud Computing Service Models

Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

Software as a Service (SaaS)

Cloud Deployment Models

Public

Private

Community

Hybrid

Cloud Service Provider (CSP)

Cloud Customer

Cloud Access Security Broker (CASB)

Regulators

Apache cloud stack

Business Requirement

Cloud App (Cloud Application)

Cloud Architect

Cloud Backup

Cloud Computing

Cloud Computing Reseller

Cloud Migration

Cloud OS

Cloud Portability

Cloud Provider

Cloud Service Broker

Cloud Storage

Cloud Testing

Community Cloud

Enterprise Application

Layered Defenses

Eucalyptus

FIPS 140-2

Trusted Cloud Initiative Reference Model

Vendor Lock in

Vendor Lock out

Virtualization

Sensitive Data

Virtualization

Encryption

Auditing and Compliance

Cloud Service Provider Contracts

Hardening Devices

Risk appetite

Avoidance

Acceptance

Transference

Mitigation

Resource pooling

Broad network access

Rapid elasticity

Measured service meters

On-demand self-service

Multitenancy

ISO/IEC 17788

NIST 500-292

APIs

Infrastructure

Metastructure

Infostructure

Applistructure

Cloud Computing

Traditional Computing

Shared responsibility model

The Consensus Assessments Initiative Questionnaire (CAIQ)

The Cloud Controls Matrix (CCM)

ISO 31000:2009

ISO/IEC 31010:2009

NIST Special Publication 800-37

**Domain 2 Cloud Data Security:**

Crypto Shredding

Proxy encryption

Hashing Technique

Data life cycle

DLP

Storage types

Data retention

Accidental loss

Data Classification

Obfuscation

Tokenization

Anonymization

Homomorphic encryption

Ephemeral swapping

Controller

Key management

Create

Store

Use

Share

Archive

Destroy

Entity

Identity

Identifier

Attributes

Persona

Role

Authentication

Multifactor Authentication (MFA)

Access control

Authorization

Entitlement

Federated Identity Management

Authoritative source

Identity Provider

Relying Party

Security Assertion Markup Language (SAML) 2.0

OAuth

OpenID

eXtensible Access Control Markup Language (XACML)

System for Cross-domain Identity Management (SCIM)

Hard tokens

Soft tokens

Out-of-band Passwords

Biometrics

**Domain 3 Terms**

Compute

Storage

Virtualization

Management plane

NFV

SDN

Reservations

Limits

Shares

SAN

NAS

Object storage

Volume storage

Hypervisor ( I and II)

Uptime institute and tiers

HVAC

TPM

Cloud orchestration

Federation

Identity provider

Relaying party

User

SAML

Oauth 2.0

OpenID

SSO

CASBs

RPO

RTO

RSL

**Domain 4 Terms:**

OWASP top 10

CSSDLC

MTD

RTO

Uptime against availability

Average uptime for CSP 99.999

SLAs

Cost benefit analysis

Standards

APIs

Devops

REST

SOAP

Training

Apps on prim Apps in the cloud

Documentation

Forklift

Define

Design

Develop

Test

Secops

Dispose

Change Management

STRIDE

IAM

DAST

SAST

SSL/TLS

SAML

Hub & Spoke Model

Free form Model

XML Gateways

Pentest/Vulnerability scanning

CSX/CSFR

Federated Identity Provider

Sandboxing

Supply chain management

ISO 27034-1

Propriety/Open source

Federation

WS Federation

Relying party

Identity provider

SSO

Single\Dual\Multifactor Authentication

ONF\ANF

ISO 28000:2007

Database activity monitoring

ACID

Test data generation

Dynamic masking

Data Masking

Sandbox

Trusted 3rd party

DAM

WAF

Create

Store

Use

Share

Archive

Destroy

Read

Process

Store

An actor

Software Development Kits (SDKs)

Command Line Interfaces (CLIs)

Software-Defined Infrastructure

Chaos Engineering

Software Defined Networking (SDN)

Microsoft’s Security Development Lifecycle

NIST 800-64

Code Review

Unit testing

regression testing

functional tests

Segregation by default

Immutable infrastructure

Increased use of micro-services

PaaS and “serverless” architectures

Software-defined security

Event driven security

Standardization

Automated testing

Immutable

Improved auditing and change management

Rugged DevOps

HSM/appliance

Virtual appliance/software

Cloud provider service

Hybrid

Security Assertion Markup Language (SAML) 2.0

OAuth

OpenID

eXtensible Access Control Markup Language (XACML)

System for Cross-domain Identity Management (SCIM)

Hard tokens

Soft tokens

Out-of-band Passwords

Biometrics

**Domain 5 Terms:**

Private Cloud on Prim own the infrastructure

Cloud provider Collaboration/SLAs

ISO 15408

EAL

Chokepoints

Host Hardening

Baselines

Documentation

Governance and compliance

Patch management

Log management

Change management

Problem management

Storage protocols

iscsi

Sans

Lun

Overconsumption

Sandboxing

3 states of data

Fault tolerance

Secure KVMs for the CSP

USB for servers and devices

Vlans

Trunking

IPSec

DNSSEC

DRS\CRS

Maintenance Mode

NIST 800-92

NIST 800-40

VM performance monitoring: CPU/Storage/Memory/Networking

Redundancy

DR\BC

Backup types: Full/Copy/Deferential/Incremental

IDS/IPS

HIPS/HIDS

Honeypot\Honeynet

Logical/physical design

ISO 28000:2007

ISO/IEC 27018

Type I\II Hypervisor

Object storage

Volume storage

Database

Application/platform

HSM/appliance

Virtual appliance/software

Cloud provider service

Hybrid

Web consoles

Identity and Access Management (IAM)

multi-factor authentication (MFA)

Perimeter security

Customer authentication

Internal authentication and credential passing

Authorization and entitlements

Logging, monitoring, and alerting

Metastructure

Software-Defined Infrastructure

Infrastructure

Infostructure

Applistructure

Chaos Engineering

SDN firewalls

Default deny

Software Defined Perimeter Working Group

hybrid connection

Second-level networks connect

Virtual machines

Platform-based workloads

Serverless computing

“Traditional” agents

File integrity monitoring

The cloud owner (public or private)

Compute

Network

Storage

Containers

Security settings

identity management

Monitoring and logging

Image asset management

dedicated hosting

Cloud Provider Responsibilities

Cloud User Responsibilities

Assuring the security of the underlying physical infrastructure

Assuring the security of the management plane

Properly securing the image repository

Building security into the tasks/code running inside the container

NIST 800-61

ISO/IEC 27035

Preparation

Detection and Analysis

Containment

Eradication and recovery

Documenting the incident and gathering evidence

Post-mortem

IaaS/PaaS vs. SaaS

Cloud jump kit

Architect the cloud environment for faster detection, investigation, and response

Object storage

Volume storage

Database

Application/platform

CASB

URL filtering

DLP

Management plane

Public and internal sharing controls

Encryption

Tokenization

IaaS Encryption

Instance-managed encryption

Externally managed encryption

Client-side encryption

Server-side encryption

Proxy encryption

PaaS encryption

Application layer encryption

Database encryption

SaaS Encryption

Provider-managed encryption

Proxy encryption

HSM/appliance

Virtual appliance/software

Cloud provider service

Hybrid

Data Loss Prevention (DLP)

Full DRM

Provider-based control

Test data generation

Dynamic masking

Managing data location/residency

**Domain 6 Legal and Compliance**:

Risk

Risk Mitigation

Risk Avoidance

Risk Transference

Risk analysis

Criminal law

International law

Conflict of law

Gap analysis

PII

HIPPA

FERPA

SOX

SOC 1

SOC 2

SOC 3

GLBA

Common Criteria

CSA

CSA STAR

CSA STAR Level 1

CSA STAR Level 2

CSA STAR Level 3

CSA CCM

ISO/IEC 27018

Directive 95/46 EC

Safe harbor

Supply-chain Management (e.g., ISO/IEC 27036)

SLA

**Frameworks, Laws, and Regulators**.

ISO/IEC 27018

ISO/IEC 27036

Directive 95/46 EC

Safe harbor

ISO/IEC 27018

ISO/IEC 27036

HIPPA

FERPA

SOX

PCI-DSS

GLBA

ISO

NIST

FTC

SEC

Criminal law

International law

Conflict of law

ISO 28000:2007

ISO 15408

NIST 800-92

NIST 800-40

ISO/IEC 27018

ISO 27034-1

NIST 800-145

NIST 800-146

NIST 800-53

FIPS 140-2

NIST 800-37

ACIPA

GDPR

ENISA

NIPA

ISO/IEC 17788

ISO/IEC 17789

NIST 500-292

CSA

Uptime Institute