Certificate of Cloud Security Knowledge

CCSK Foundation Student Handbook

Version 4.1

Released November, 2019

© 2019 Securosis, LLC and Cloud Security Alliance.
All Rights Reserved.

CERTIFICATE OF CLOUD SECURITY KNOWLEDGE FOUNDATION & PLUS

CREATED BY SECUROSIS, LLC FOR THE CLOUD SECURITY ALLIANCE

1

Course Objective

To provide students with a base of knowledge on cloud computing security theory and practice and assist students in taking the CCSK exam.

CSA cloud security alliance®

2

INSTRUCTOR LOGO HERE
Change img on all slide masters.

2

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Course Overview

The CCSK Foundation Course will prepare you for the CCSK exam and provide additional material and context.

To pass the exam, you will still need to study the CSA Guidance, the Cloud Controls Matrix (CCM), and the ENISA Risk Report.

The content is found in the CSA Guidance, and will be updated as the guidance evolves.

cloud security alliance®

3

INSTRUCTOR LOGO HERE
Change img on all slide masters.

3

The **CCSK Plus course** will prepare you for the CCSK exam and provides expanded material and exercises to grow your practical knowledge of cloud computing security through hands-on exercises.

To pass the exam you will still need to study **the CSA Guidance, Common Assessment Initiative Questionnaire (CAIQ), the Cloud Controls Matrix (CCM)** and **the ENISA risk report.**

cloud security alliance®

4

INSTRUCTOR LOGO HERE
Change img on all slide masters.

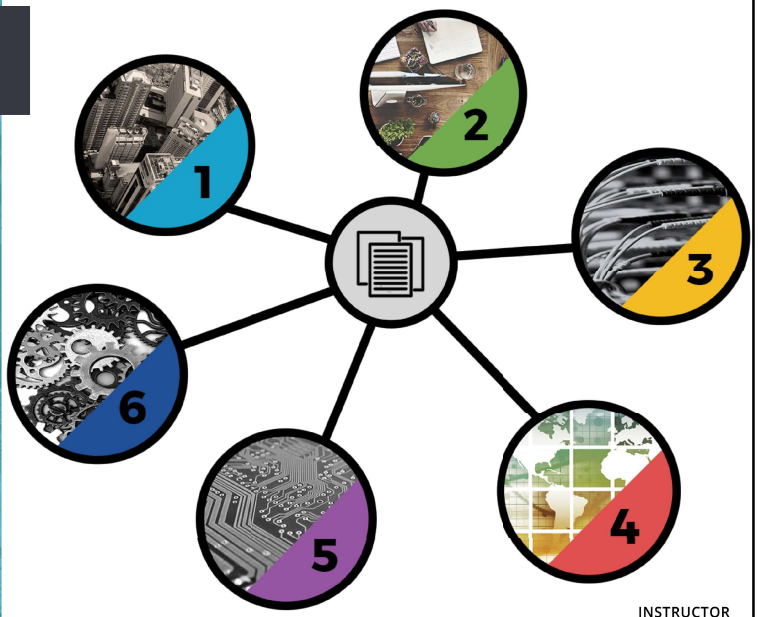
4

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Course Structure

The CCSK Foundation Training is divided into 6 modules which map to domains outlined in the CSA Security Guidance. Find out more by hovering over the circles on the right.

DOWNLOAD THE LATEST VERSION OF THE CSA SECURITY GUIDANCE.



5

INSTRUCTOR LOGO HERE
Change img on all slide masters.

5

Course Structure

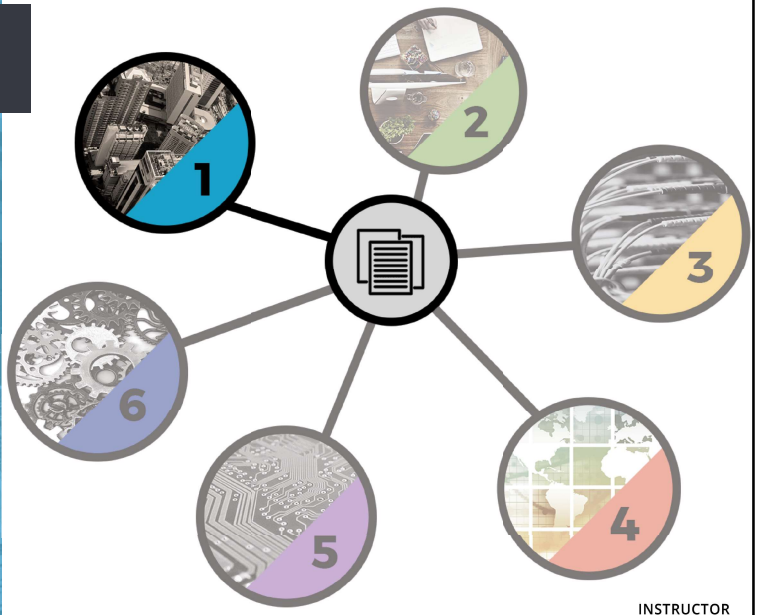
MODULE 1 //
Introduction To Cloud Computing

Maps to the following domains in the Security Guidance:

Domain 1 // Cloud Computing Concepts and Architectures

Covers the following subject areas:

- NIST
- Essential characteristics
- Service models
- Deployment models



6

INSTRUCTOR LOGO HERE
Change img on all slide masters.

6

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Course Structure

MODULE 2 //
Infrastructure Security For Cloud

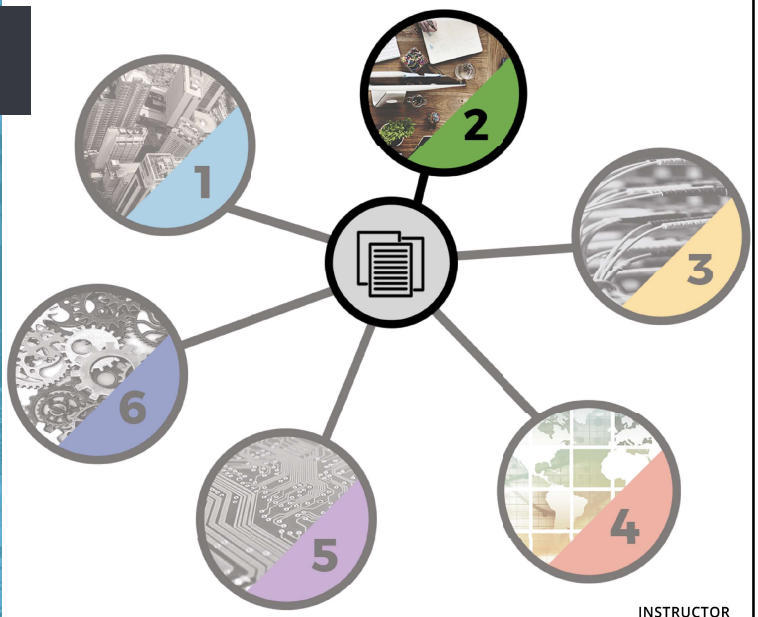
Maps to the following domains in the Security Guidance:

- **Domain 6 //** Management Plane and Business Continuity
- **Domain 7 //** Infrastructure Security
- **Domain 8 //** Virtualization and Containers

Also maps to CAIQ and CCM, and ENISA

Covers the following subject areas:

- Securing base infrastructure
- Management plane security
- Securing virtual hosts and networks
- IaaS, PaaS, SaaS security



cloud security alliance®

7

INSTRUCTOR LOGO HERE
Change img on all slide masters.

7

Course Structure

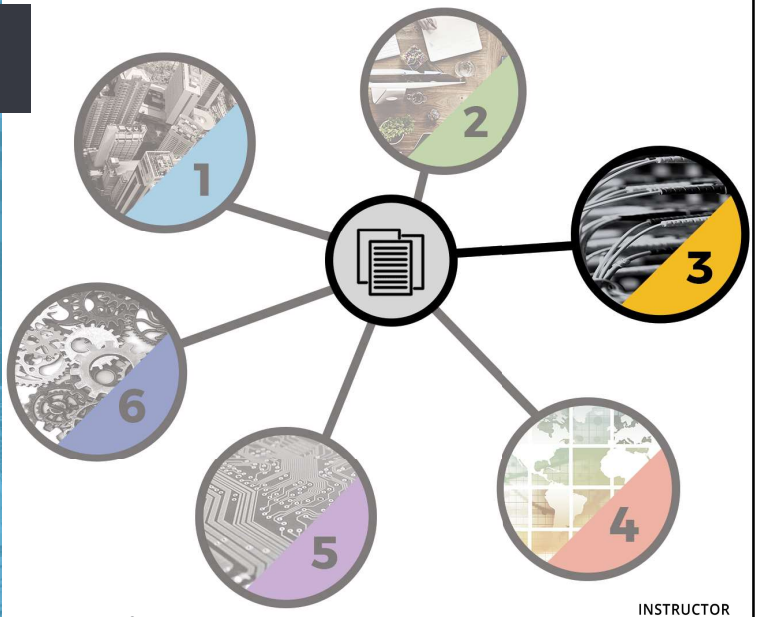
MODULE 3 //
Managing Cloud Security & Risk

Maps to the following domains in the Security Guidance:

- **Domain 2 //** Governance and Enterprise Risk Management
- **Domain 3 //** Legal Issues, Contracts and Electronic Discovery
- **Domain 4 //** Compliance and Audit Management
- **Domain 5 //** Information Governance

Covers the following subject areas:

- Risk and governance
- Legal and compliance
- Audit
- Data governance



cloud security alliance®

8

INSTRUCTOR LOGO HERE
Change img on all slide masters.

8

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Course Structure

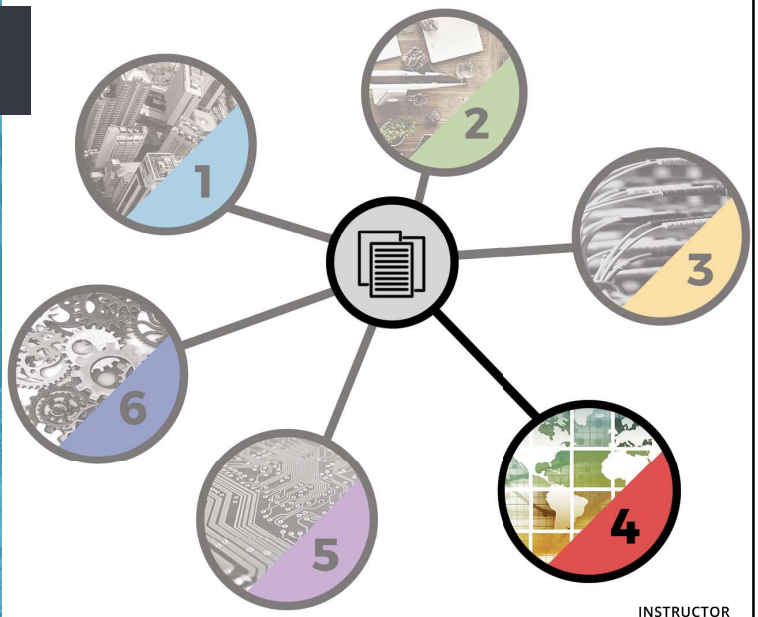
MODULE 4 //
Data Security For Cloud
Maps to the following domains in the Security Guidance:

Domain 6 // Management Plane and Business Continuity

Domain 11 // Data Security

Covers the following subject areas:

- Cloud data architectures
- Data security and encryption
- CASB and data loss prevention
- BC/DR



cloud security alliance®

9

INSTRUCTOR LOGO HERE
Change img on all slide masters.

9

Course Structure

MODULE 5//
Securing Cloud Applications, Users & Related Technologies
Maps to the following domains in the Security Guidance:

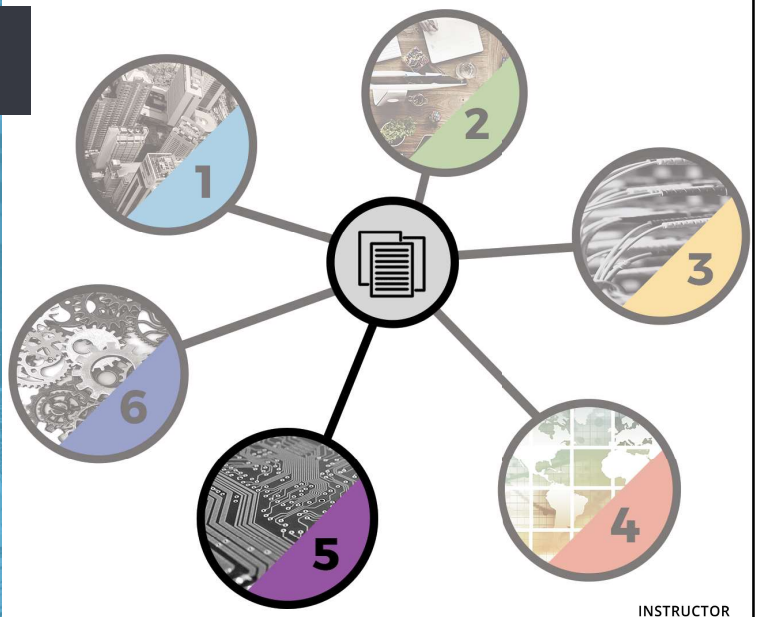
Domain 10 // Application Security

Domain 12 // Identity Entitlement and Access Management

Domain 14 // Related Technologies

Covers the following subject areas:

- Application security
- Identity and access management
- Related technologies



cloud security alliance®

10

INSTRUCTOR LOGO HERE
Change img on all slide masters.

10

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Course Structure

MODULE 6 // Cloud Security Operations

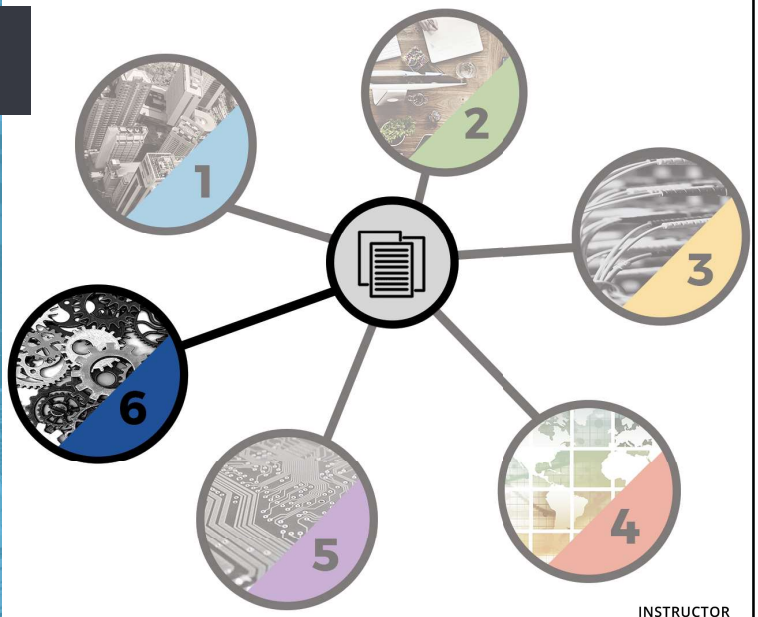
Maps to the following domains in the Security Guidance:

Domain 9 // Incident Response

Domain 13 // Security as a Service

Covers the following subject areas:

- What to look for in a cloud provider
- Security as a Service
- Incident Response



cloud security alliance®

11

INSTRUCTOR LOGO HERE
Change img on all slide masters.

11

Note

- If you are taking the CCSK Plus class and have not subscribed to Amazon EC2 and followed the pre-class setup instructions, you need to *now*.
  - It can take up to a day for your EC2 credentials to fully activate, but it typically happens within minutes.

cloud security alliance®

12

INSTRUCTOR LOGO HERE
Change img on all slide masters.

12

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Learning Outcomes

1. Be prepared to successfully pass the CCSK written exam.
2. Understand cloud models and architectures, and how to apply the Shared Responsibilities model to building a cloud security program.
3. Know the impacts of cloud computing on governance, legal, risk, and regulatory compliance.
4. Learn to adapt existing security principles and practices for cloud deployments, including the impact of cloud on all traditional security domains.
5. Be able to practically apply the Cloud Security Alliance Security Guidance, Cloud Controls Matrix, and other research to a cloud security program.

cloud security alliance

13

INSTRUCTOR LOGO HERE
Change img on all slide masters.

13

INTRODUCTION AND CLOUD ARCHITECTURES

MODULE 1

14

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Module Structure

Content in this module comes from the following domains in CSA's Security Guidance and covers the following subject areas:

Domain 1 // Cloud Computing Concepts and Architectures

- NIST
- Essential characteristics
- Service Models
- Deployment models

Click on the circle to the right to view the unit outline.

DOWNLOAD THE LATEST VERSION OF THE CSA SECURITY GUIDANCE.

cloud security alliance®

15

INSTRUCTOR LOGO HERE
Change img on all slide masters.

15

Module Structure

Unit 1 // Module Intro

Unit 2 // Introductions to Architecture

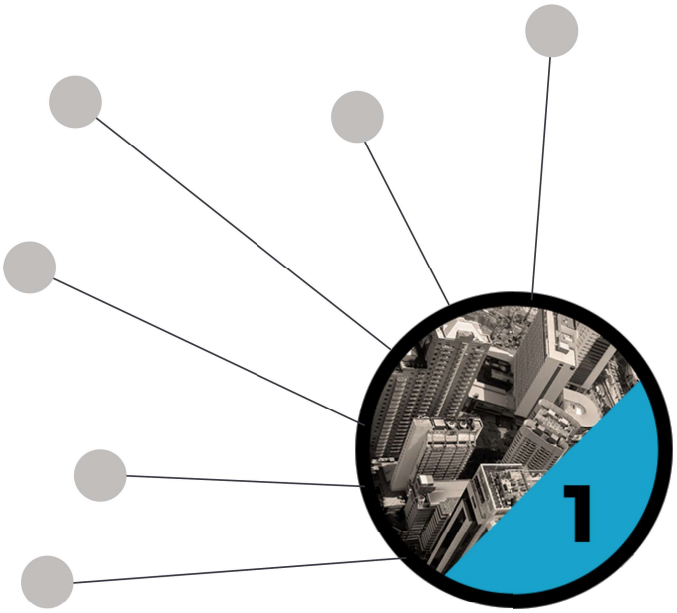
Unit 3 // Cloud Essential Characteristics

Unit 4 // Cloud Service Models

Unit 5 // Cloud Deployment Models

Unit 6 // Shared Responsibilities

cloud security alliance®



16

INSTRUCTOR LOGO HERE
Change img on all slide masters.

16

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Learning Objectives

Understand the components of cloud infrastructure

Assess the security implications of virtual networks and workloads

Learn the security advantages of disadvantages of working with cloud infrastructure

Evaluate how to secure the cloud management plane

Learn how to manage business continuity for cloud computing

cloud security alliance®

17

INSTRUCTOR LOGO HERE
Change img on all slide masters.

17

The Amazon EC2 Story

Amazon wanted to more efficiently use their resources.

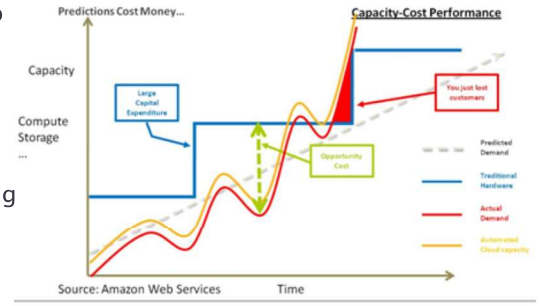
- And better enable developers without having to go through hardware procurement.

Cloud meant they didn't have to have dedicated capacity for each kind of system.

- Just pull what's needed out of the pool.
- Still needed enough overall capacity for peak (e.g. holidays), so a lot of hardware wasn't being used day to day.

Rent out the spare capacity (EC2).

- Note that public AWS was a separate project, NOT renting core capacity, but all Amazon now runs on it.



cloud security alliance®

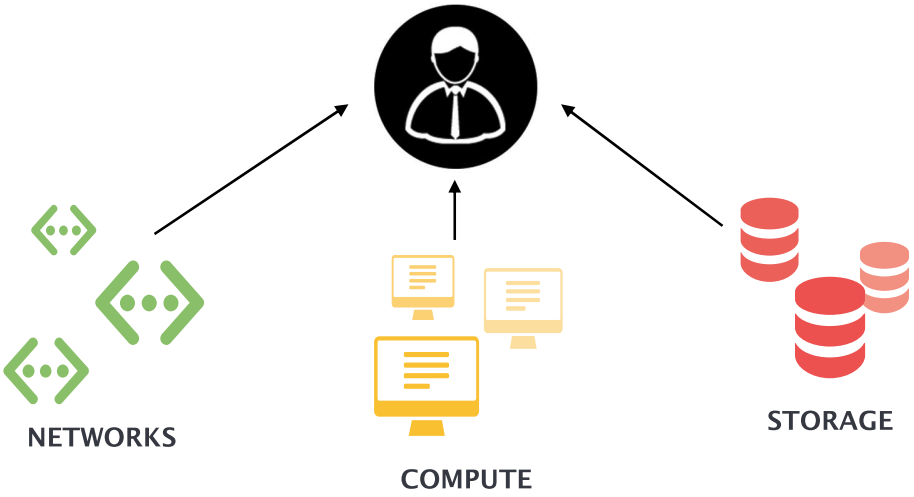
18

INSTRUCTOR LOGO HERE
Change img on all slide masters.

18

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Resource Pools



19

Building Resource Pools

ABSTRACTION

AUTOMATION

20

Copyright 2019 Cloud Security Alliance and Securosis, LLC

"Static" Virtualization vs. Cloud Computing

Traditional virtualization

- Abstraction of compute, network, and storage from physical infrastructure.
- A human administrator *manually (mostly) allocates resources.*
- Not self-service. Administrator required.
- Not *elastic* due to lack of automation.

Cloud computing

- Abstraction of compute, network, storage (and more) from physical infrastructure.
- The cloud *automates and orchestrates* management of the resource pools.
- Self-service. Users provision the resources from their own allocated pool based on policies.

CSA cloud security alliance®

21

INSTRUCTOR LOGO HERE
Change img on all slide masters.

21

What is Cloud Computing?

- Cloud separates application and information resources from the underlying infrastructure, and the mechanisms used to deliver them.
- Cloud describes the use of a collection of services, applications, information, and infrastructure comprised of pools of compute, network, information, and storage resources.
- These pools can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down.
- Cloud provides for an on-demand utility-like model of allocation and consumption.

CSA cloud security alliance®

22

INSTRUCTOR LOGO HERE
Change img on all slide masters.

22

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Definitions

NIST

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of conjurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

ISO IEC

Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

CSA cloud security alliance®

23

INSTRUCTOR LOGO HERE
Change img on all slide masters.

23

Potential Benefits of Cloud Computing

- No capital expenditures (using public cloud)
- More agility
- Unbounded scale
- Improved resource utilization
- Customer-controlled migration
- Resilience
- Pay for use

CSA cloud security alliance®

24

INSTRUCTOR LOGO HERE
Change img on all slide masters.

24

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. Cloud computing is a new operational model that combines the benefits of abstraction (virtualization) and automation (orchestration) for new ways of delivering and consuming technology.
2. Abstraction separates resources from their underlying physical infrastructure. It allows us to create resource pools out of those underlying assets.
3. Automation (orchestration) allows us to rapidly provision and deprovision those resources from the resource pool.
4. This is different than traditional virtualization which includes the abstraction piece, but doesn't necessarily use that to build resource pools, and lacks the advanced orchestration of cloud.
5. Cloud can potentially provide a wide range of benefits, but the key ones are economic, agility, and resiliency.

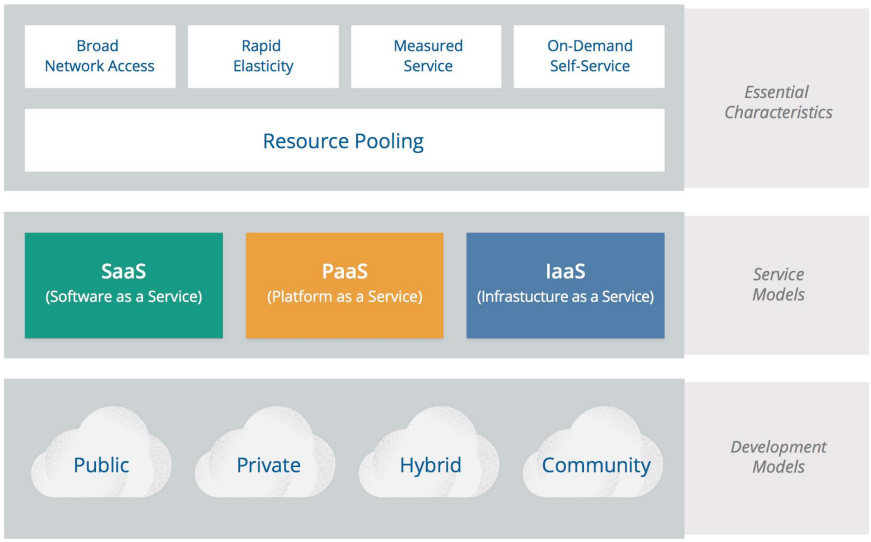
cloud security alliance

25

INSTRUCTOR LOGO HERE
Change img on all slide masters.

25

NIST Model of Cloud Computing



cloud security alliance

26

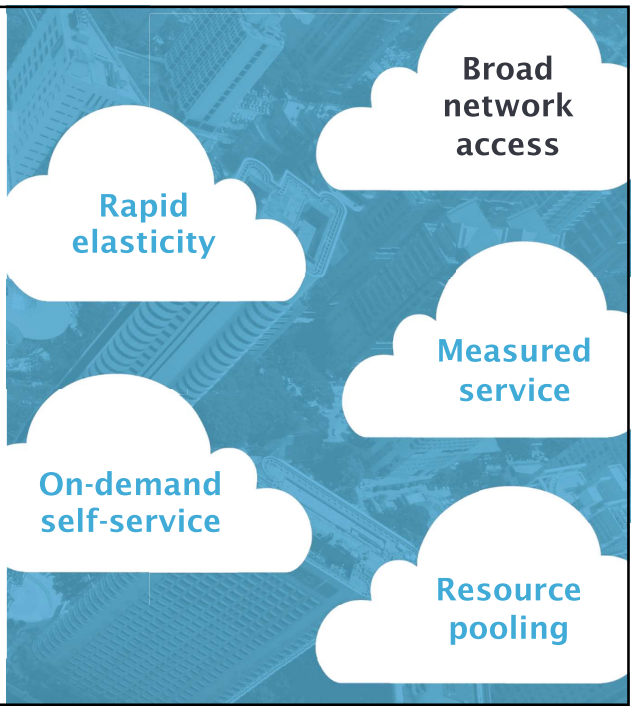
INSTRUCTOR LOGO HERE
Change img on all slide masters.

26

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Broad Network Access

- Access through standard clients
  - Computers (desktops, laptops)
  - Mobile devices
- Traditional or cloud-based software services (applications, processes, etc.)



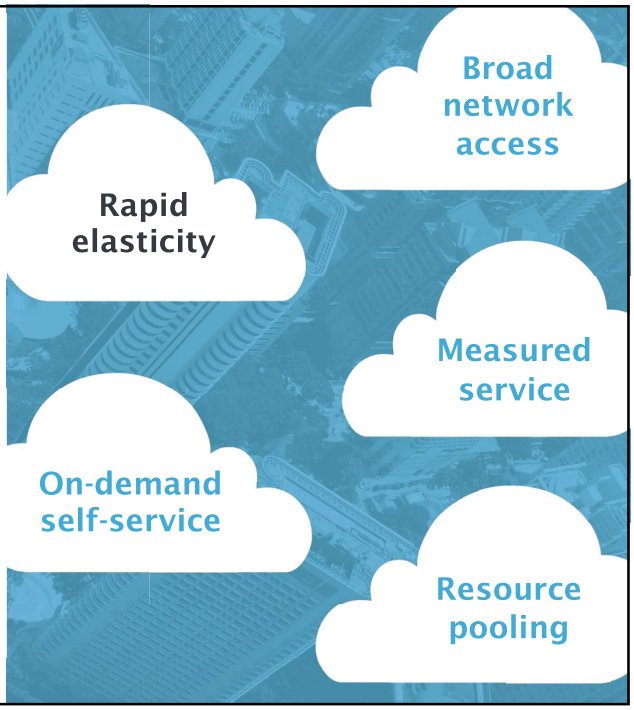
CSA cloud security alliance®

27

27

Rapid Elasticity

- Services can be rapidly and elastically provisioned - in some cases, automatically - to quickly scale out; and rapidly released to quickly scale in.



CSA cloud security alliance®

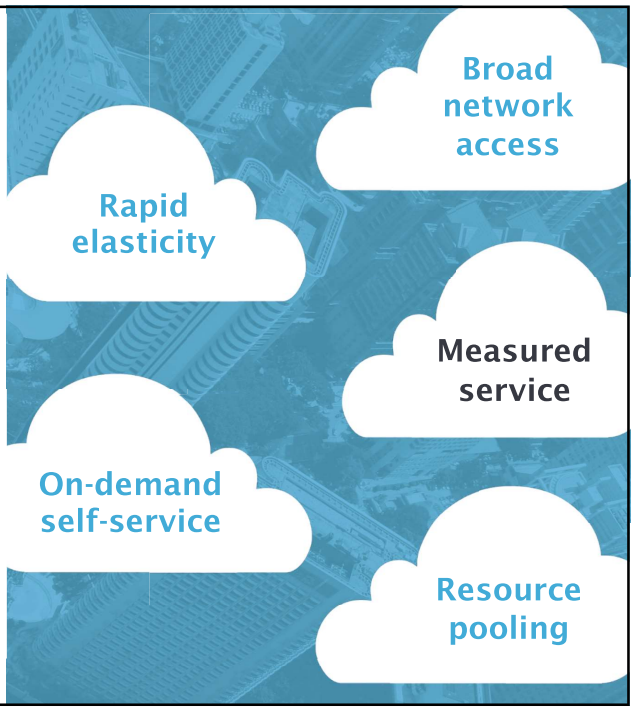
28

28

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Measured Service

- Automatically control and optimize resource usage
- Leveraging a metering capability at some level of abstraction
- Utility computing - you pay for what you use.



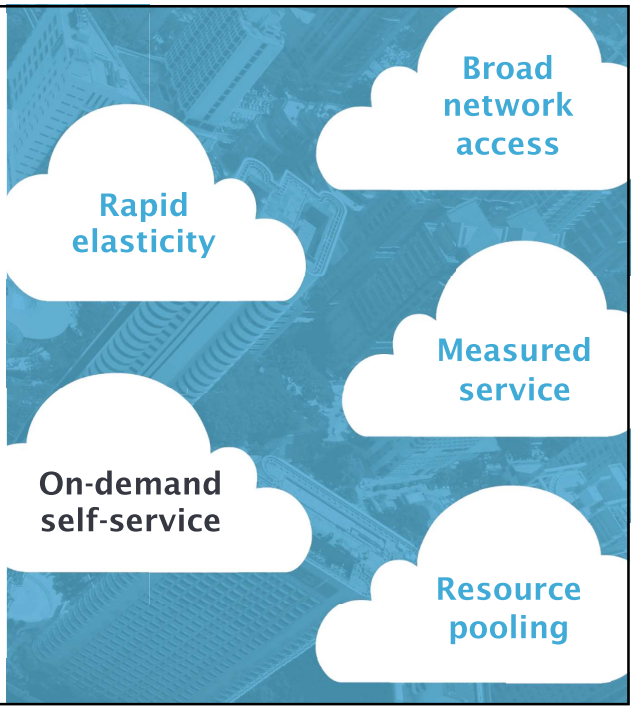
cloud security alliance®

29

29

On-Demand Self-Service

- A consumer can unilaterally provision computing capabilities, such as server time and network storage as needed automatically, without requiring human interaction with a service provider.



cloud security alliance®

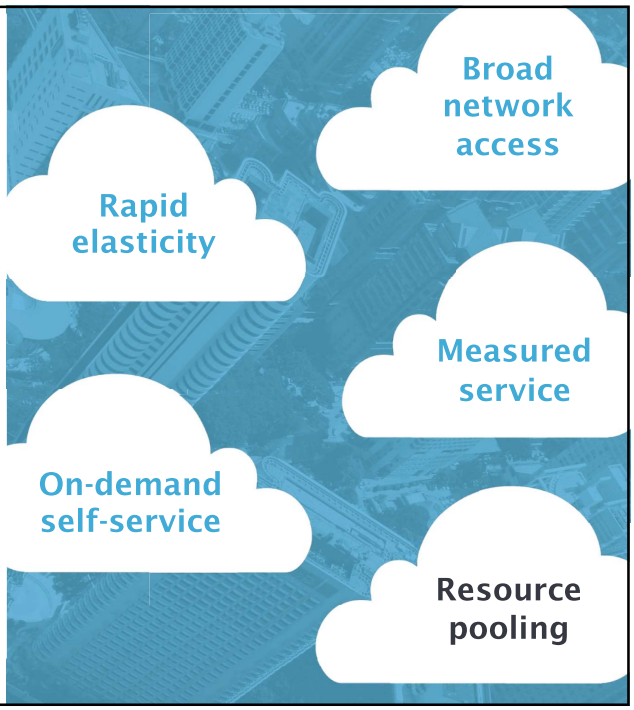
30

30

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Resource Pooling

- Resources are pooled to serve multiple consumers using a multi-tenant model
  - Different physical and virtual resources
- Location independence
  - Exact location of resources not in customer's control



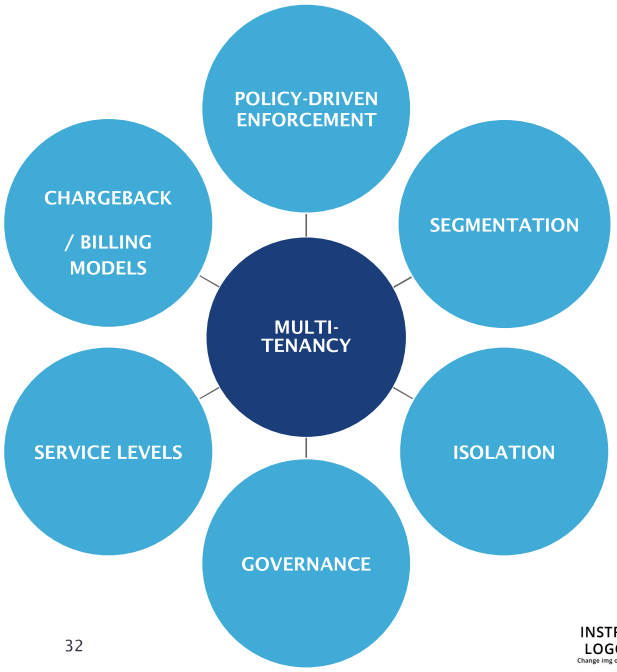
cloud security alliance®

31

31

Resource Pooling & Multitenancy

Multi-tenancy is an emergent property of resource pooling. Once you have a pool and allow more than one consumer to access it, you have multitenancy. For multitenancy of a shared resource pool to work it needs a few characteristics and enforcement capabilities; all of which affect security



cloud security alliance®

32

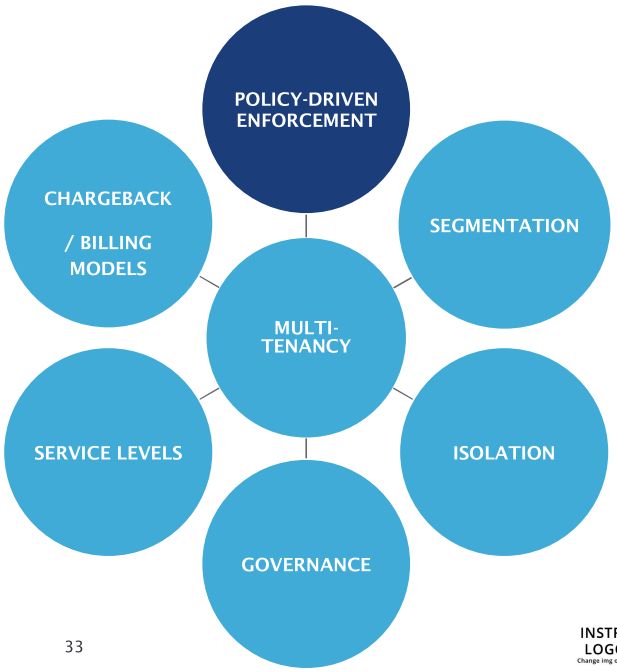
INSTRUCTOR LOGO HERE
Change img on all slide masters.

32

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Policy-Driven Enforcement

Policy-driven enforcement - the cloud provider and cloud consumers define how their environment should look and run using policies. These can be implemented in a user interface or directly via policies encoded using a formal policy language (code).



cloud security alliance®

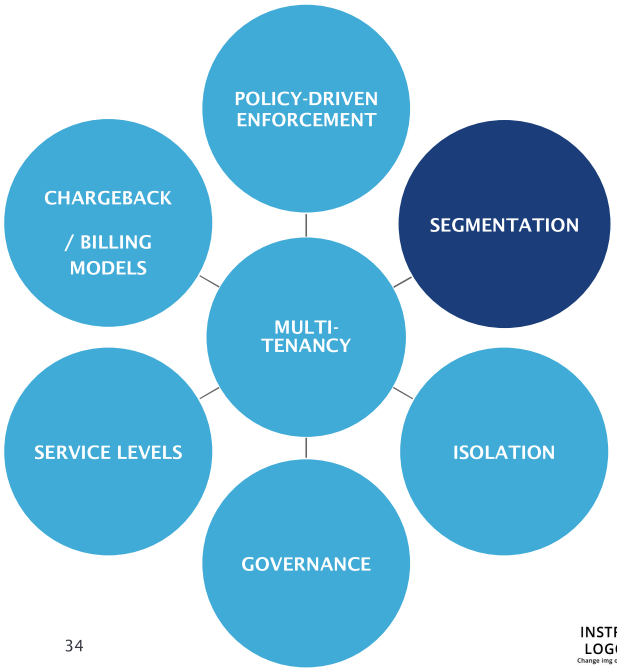
33

INSTRUCTOR LOGO HERE
Change img on all slide masters.

33

Segmentation

Customers run in their own "segment" of the cloud. Segmentation is how the provider divides the cloud up among different tenants.



cloud security alliance®

34

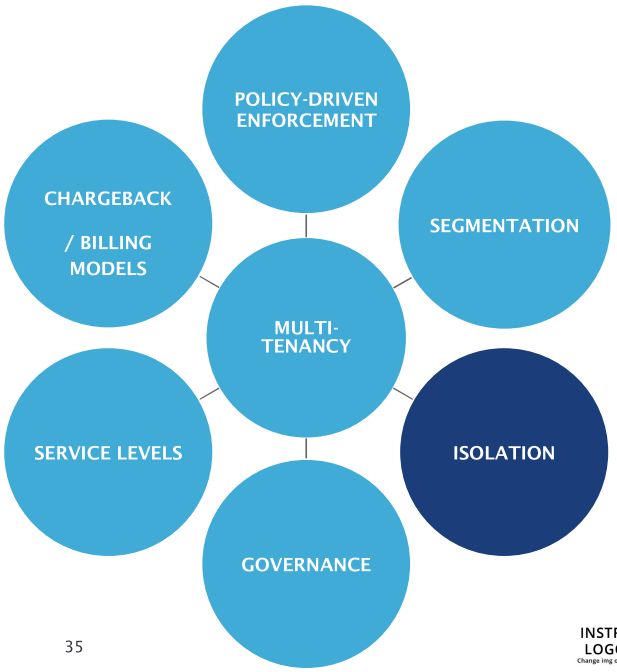
INSTRUCTOR LOGO HERE
Change img on all slide masters.

34

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Isolation

Consumers in one segment should never see anything running another segment. This is the core control that allows multiple tenants to safely share a resource pool without seeing or impacting each others' deployments.



cloud security alliance®

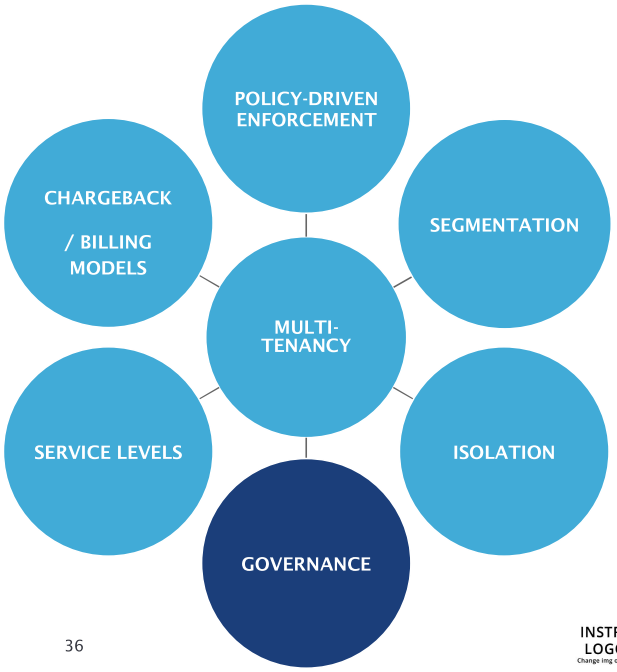
35

INSTRUCTOR LOGO HERE
Change img on all slide masters.

35

Governance

Governance is the overall management model of the cloud, from contracts and service levels to policies. Many of the other characteristics are enforcement mechanisms of governance.



cloud security alliance®

36

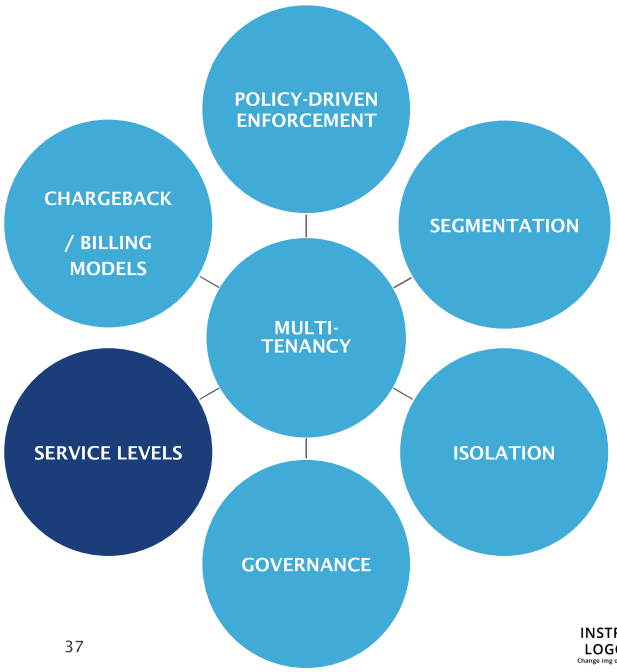
INSTRUCTOR LOGO HERE
Change img on all slide masters.

36

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Service Levels

Since a resource pool is a shared environment, the cloud provider needs mechanisms to divvy up the resources among tenants and assure them that they will have the resources that are promised. Service levels define who gets what resources.



cloud security alliance®

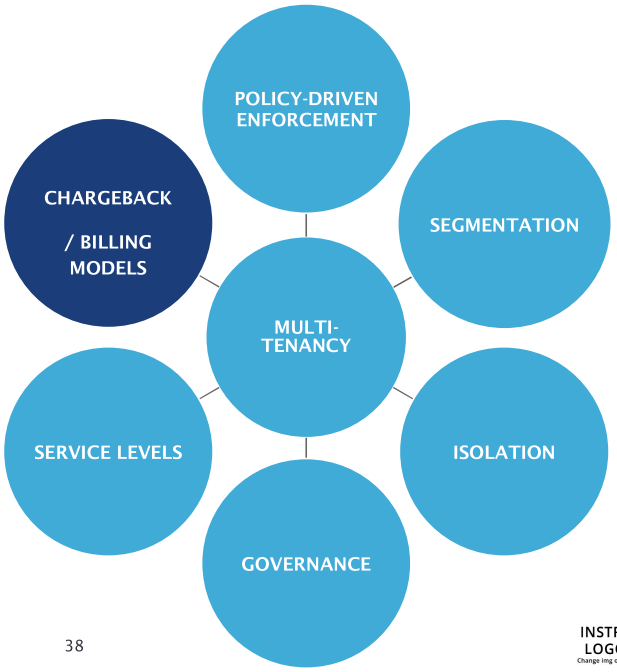
37

INSTRUCTOR LOGO HERE
Change img on all slide masters.

37

Chargeback/Billing Models

Since the cloud controller needs to know exactly who is using what resources from the pool at all times, it is only natural this is metered and can be used for billing purposes.



cloud security alliance®

38

INSTRUCTOR LOGO HERE
Change img on all slide masters.

38

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. The NIST model of cloud computing cleanly describes the essential characteristics required for something to be considered "a cloud“
2. The most important of those is resource pooling, which is what allows multiple consumers to share the same underlying physical resources.
3. But broad network access, elasticity, measured service, and self service are all also important and essential cloud features.
4. Thus multitenancy is an emergent properly of resource pooling, not an essential characteristic itself.
5. For multitenancy to work it needs strong segregation (breaking up the environment) and isolation (the security boundary between segments)

cloud security alliance®

39

INSTRUCTOR LOGO HERE
Change Img on all slide masters.

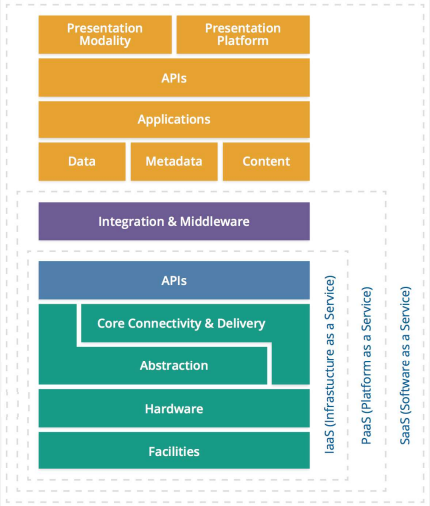
39

Cloud Service Models (SPI)

SOFTWARE AS A SERVICE
(SaaS)

PLATFORM AS A SERVICE
(Paas)

INFRASTRUCTURE AS A SERVICE
(IaaS)



cloud security alliance®

40

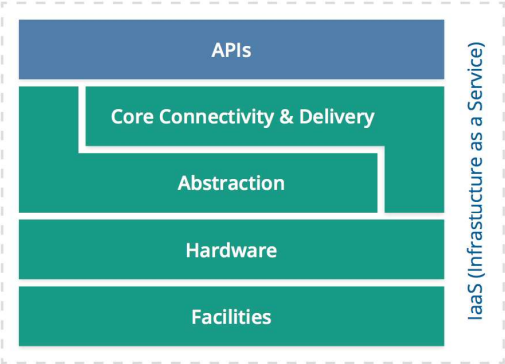
INSTRUCTOR LOGO HERE
Change Img on all slide masters.

40

Copyright 2019 Cloud Security Alliance and Securosis, LLC

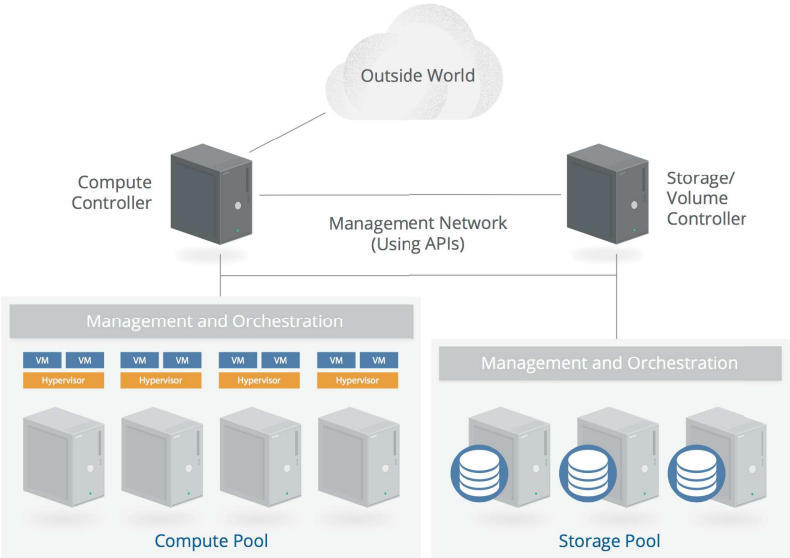
Infrastructure As A Service (IaaS)

- Provisions processing, storage, networks, and other fundamental computing resources
- Consumer deploys and runs arbitrary software
- Can include operating systems and applications



41

Simplified IaaS Architecture

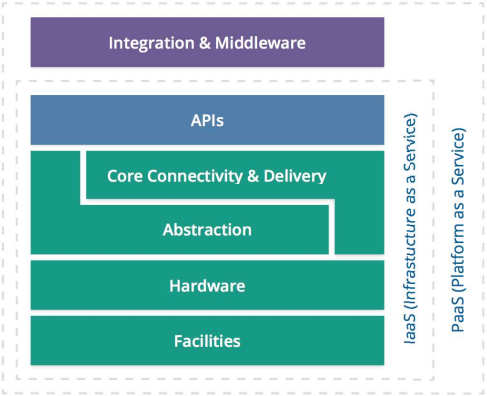


42

Copyright 2019 Cloud Security Alliance and Securosis, LLC

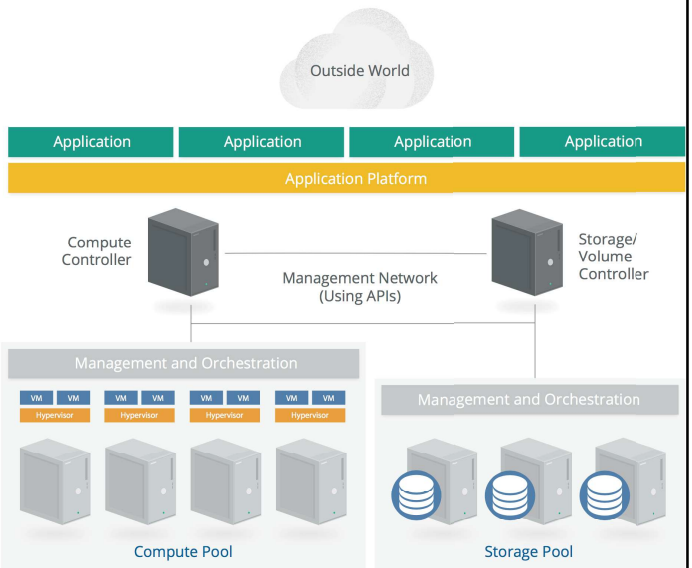
Platform As A Service (PaaS)

- Application development frameworks, middleware capabilities, and functions such as databases, messaging, and queuing.
- Deploy consumer-created or acquired applications onto cloud infrastructure
- Created using programming languages and tools supported by the cloud provider



43

Simplified PaaS Architecture

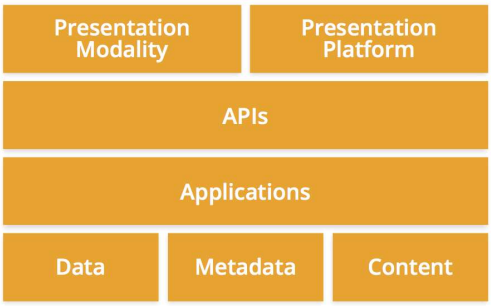


44

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Software As A Service (SaaS)

- The consumer uses the provider's applications.
- Doesn't necessarily have to run on IaaS or PaaS, but must still have the Essential Characteristics.
- The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities.



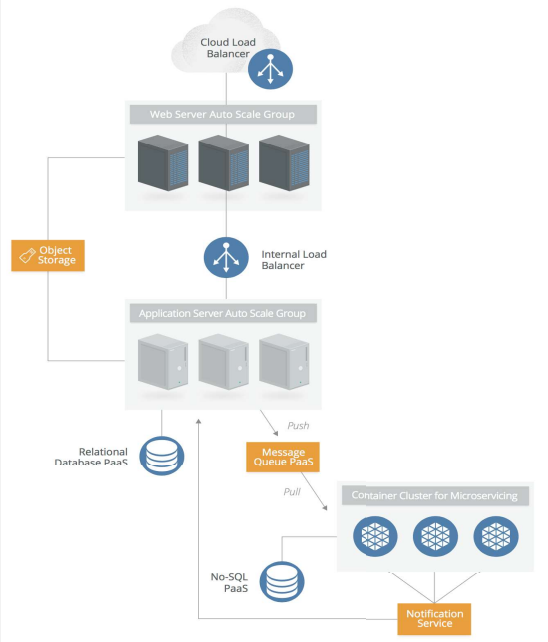
cloud security alliance®

45

INSTRUCTOR LOGO HERE
Change img on all slide masters.

45

Simplified SaaS Example Architecture



cloud security alliance®

46

INSTRUCTOR LOGO HERE
Change img on all slide masters.

46

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. Service models describe what is offered to a cloud consumer- infrastructure, a platform, or a complete application (software).
2. Infrastructure as a Service provides resource pools of virtualized infrastructure, such as compute, network, or storage pools.
3. Platform as a Service further abstracts capabilities and provides resource pools of pre-configured services where the cloud consumer doesn't manage the underlying infrastructure. PaaS includes services such as databases, container platforms, message queues, and a wide range of other options.
4. Software as a Service fully abstracts everything except the application itself. Cloud consumers use the application but have no insight or management of the underlying resources.
5. In real-world deployments cloud consumers often mix and match the service models to meet project requirements.

cloud security alliance

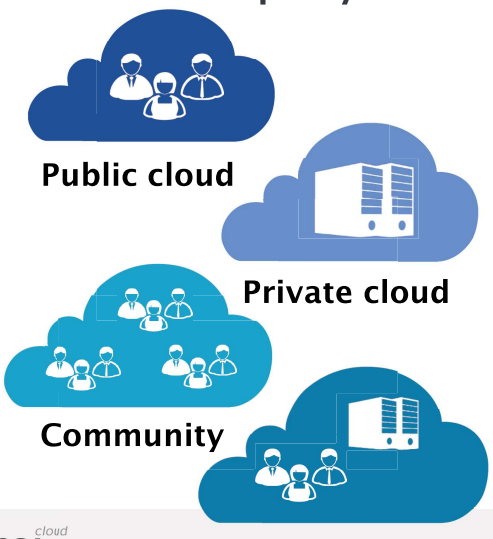
47

INSTRUCTOR LOGO HERE
Change img on all slide masters.

47

Cloud Deployment Models

Public Cloud



The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. This tends to be what most organizations view as the "cloud." Basically a big set of computers in the sky that can be spun up or decommissioned instantly to support almost any kind of applications.

cloud security alliance

48

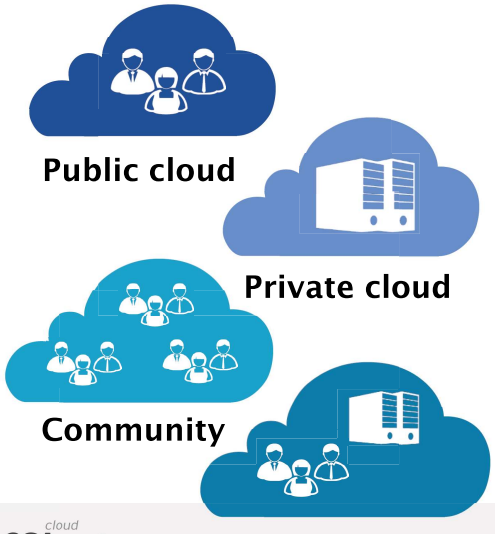
INSTRUCTOR LOGO HERE
Change img on all slide masters.

48

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Cloud Deployment Models

Private Cloud



The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party and may exist on-premises or off- premises. Any infrastructure you are responsible for managing can be termed a "private cloud." Thus your existing data center, given some of the essential characteristics of cloud infrastructure (broad network access, rapid elasticity, etc.) is sort of a private cloud. Of course, there is a lot of work to be done to turn a traditional existing data center into a private cloud facility, but it's definitely a direction many organizations are moving towards.

CSA cloud security alliance®

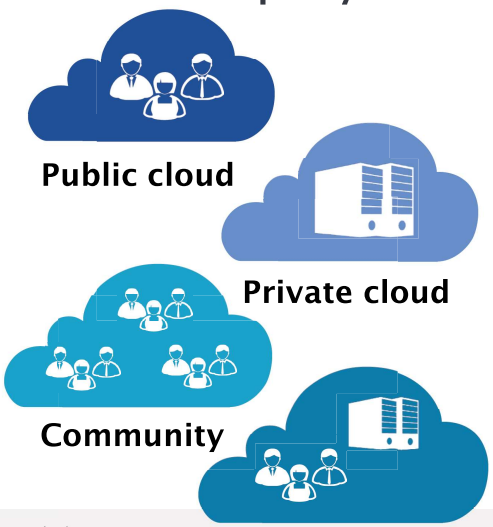
49

INSTRUCTOR LOGO HERE
Change img on all slide masters.

49

Cloud Deployment Models

Community



The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. This tends to be what most organizations view as the "cloud." Basically a big set of computers in the sky that can be spun up or decommissioned instantly to support almost any kind of applications.

CSA cloud security alliance®

50

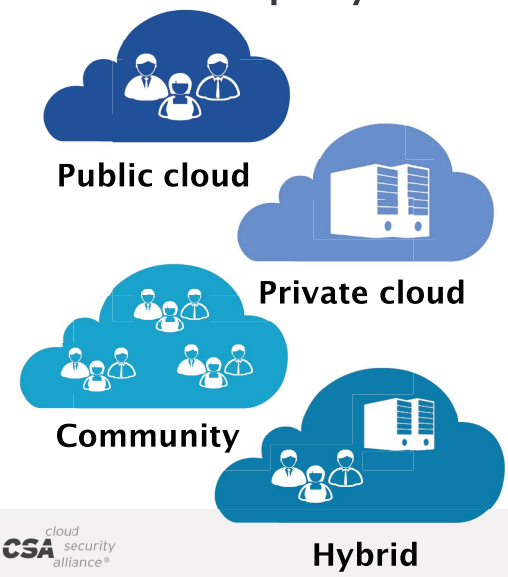
INSTRUCTOR LOGO HERE
Change img on all slide masters.

50

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Cloud Deployment Models

Hybrid



The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds). Why have one, when you can have two for twice the price? Okay, that may be a little facetious, but hybrid models are real and provide both a shorter term migration plan (so you can support your existing data centers/private cloud, while moving some or all of your infrastructure to another cloud platform).

CSA cloud security alliance®

51

INSTRUCTOR LOGO HERE
Change img on all slide masters.

51

Cloud Deployment Models & Responsibilities

	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Organization / Third Party Provider	Organization / Third Party Provider	On-Premise / Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

CSA cloud security alliance®

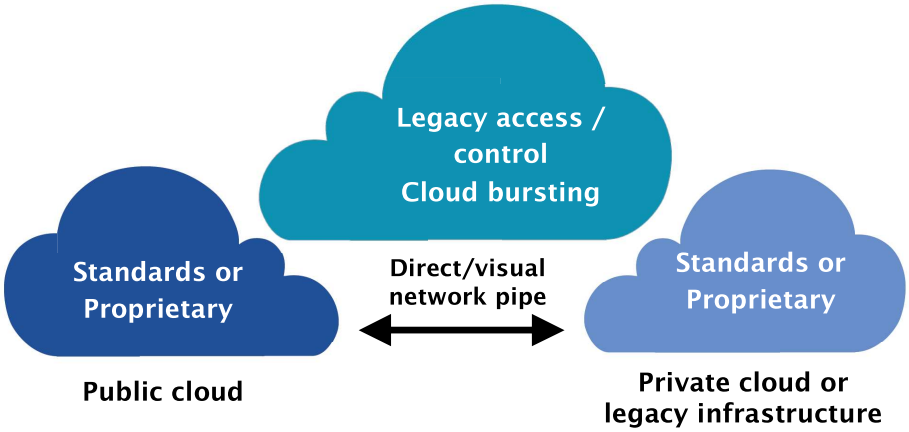
52

INSTRUCTOR LOGO HERE
Change img on all slide masters.

52

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Hybrid Cloud

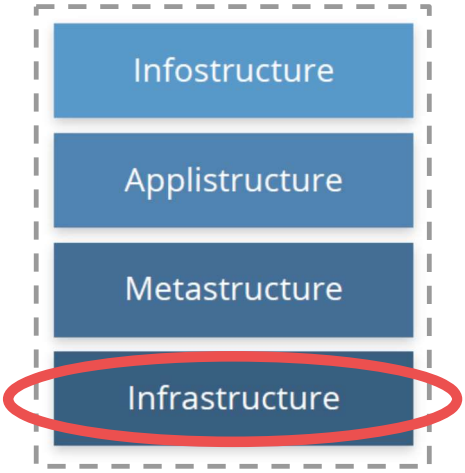


53

Logical Model

INFRASTRUCTURE

The core components of a computing system: **compute, network,** and **storage**. The foundation that every else is built on. The moving parts.



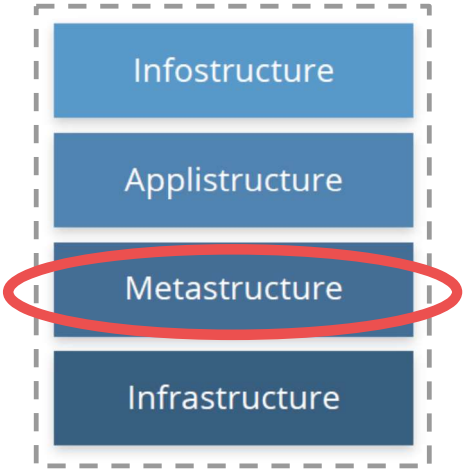
54

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Logical Model

METASTRUCTURE

The protocols and mechanisms that provide the interface between the infrastructure layer and the other layers. The glue that ties the technologies and enables management and configuration.

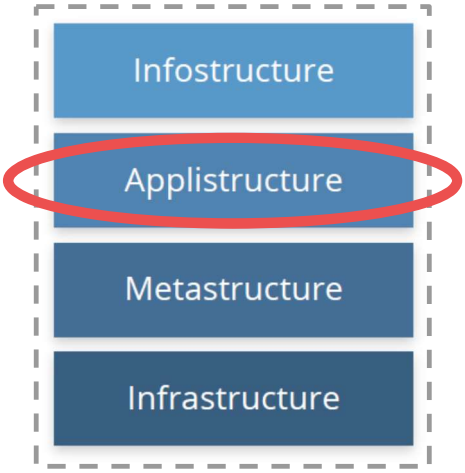


55

Logical Model

APPLISTRUCTURE

The applications deployed in the cloud and the underlying application services used to build them. For example, platform as a service features like message queues, artificial intelligence analysis, or notification services.



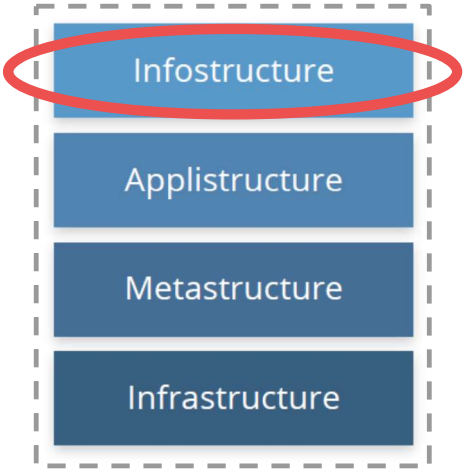
56

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Logical Model

INFOSTRUCTURE

The data and information. Content in a database, i.e. storage, etc.



cloud security alliance®

57

INSTRUCTOR LOGO HERE
Change img on all slide masters.

57

Review

1. Deployment models describe how the cloud (regardless of service model) is offered to consumers. The easiest way to think about it is "who gets to use the cloud?"
2. Public clouds are open to anyone who signs up for the service, which means different cloud consumers do not know or trust each other and the cloud provider is responsible for keeping them isolated.
3. Private and community clouds are reserved only for trusted users; those from the same organization or a group of trusted organizations. Someone else can still own and operate the cloud, but only the trusted users are allowed.

   Hybrid cloud connects on premise resources to a public cloud deployment.
4. The logical model is a different way to describe how we distribute our resources and application components. It is useful in showing how data, infrastructure, application and management components are organized across environments.
5.

cloud security alliance®

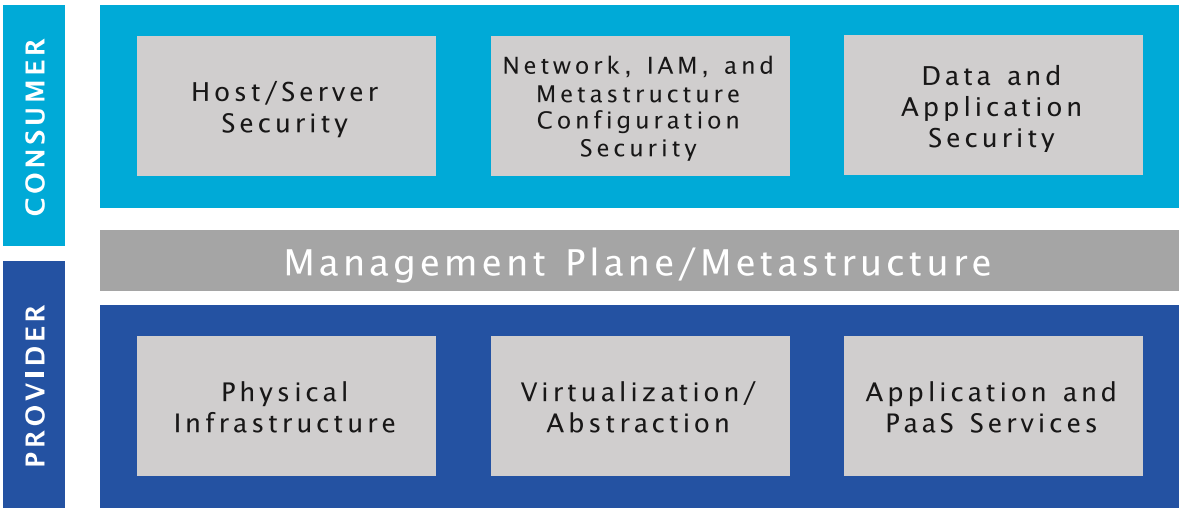
58

INSTRUCTOR LOGO HERE
Change img on all slide masters.

58

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Shared Responsibilities Model



cloud security alliance

59

INSTRUCTOR LOGO HERE
Change img on all slide masters.

59

Security Impact of the Service Model

The lower down the stack the cloud service provider stops, the more security capabilities and management consumers are responsible for implementing and managing themselves.

cloud security alliance

60

INSTRUCTOR LOGO HERE
Change img on all slide masters.

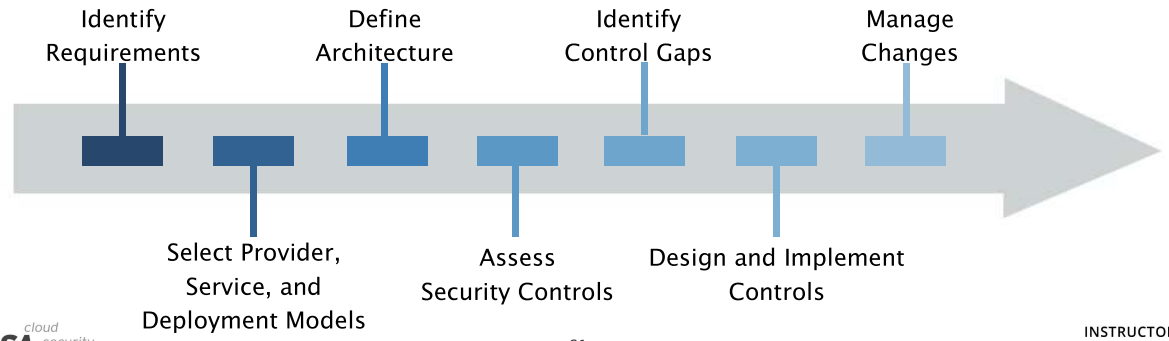
60

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Cloud Security

SECURITY CONSIDERATIONS BREAK DOWN TO:

- How does the underlying technology affect security controls?
- Who will consume assets, resources, information?
- Who is responsible for governance, security, and compliance?



cloud security alliance®

61

INSTRUCTOR LOGO HERE
Change img on all slide masters.

61

Conclusion

1. Cloud describes the use of pools of compute, network, information, and storage resources.
2. Characteristics of cloud services include:
   broad network access, rapid elasticity, measured service, on-demand self service, and resource pooling
3. Cloud services tend to be delivered as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS), though the distinctions are blurring.
4. Cloud services can be deployed as public, private, hybrid or community clouds depending on the security and sharing requirements of the application.

cloud security alliance®

62

INSTRUCTOR LOGO HERE
Change img on all slide masters.

62

Copyright 2019 Cloud Security Alliance and Securosis, LLC