



**#SysAdminDay**  
Virtual Event  
July 29, 2022



**#SysAdminDay**

Virtual Event

July 29, 2022

# How CSA help shaping proper cloud services through CCSK and CCM

Tanat Tonguthaisri

<https://LinkedIn.com/in/epicure/>



**#SysAdminDay**

Virtual Event

July 29, 2022

# How CSA help shaping properly **secured** cloud services through CCSK and CCM

Tanat Tonguthaisri  
<https://LinkedIn.com/in/epicure/>

# Agenda

- (1) In your current role at xxxx, as a xxxx, you do xxx (insert your job description). Can you tell us about what your job involves?
- (2) Can you share with us some complexities in managing cloud computing projects?
- (3) In managing (outsourced) cloud projects, what are useful tips you could share with IT professionals to avoid common pitfalls?
- (4) What made you decide to earn your CCSK? What part of the material from the CCSK has been the most relevant in your work and why?
- (5) How does CCM help communicate with customers?
- (6) What's the value in a vendor-neutral certificate like the CCSK or CCSP versus getting certified by AWS? In what scenario are the different certificates important?
- (7) Would you encourage your staff and/or colleagues to obtain CCSK or other CSA qualifications? Why?
- (8) What is the best advice you will give to IT professionals in order for them to scale new heights in their careers?



The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment.

# Days of Future Past

(1) In your current role at xxxx, as a xxxx, you do xxx (insert your job description). Can you tell us about what your job involves?

# Next Endeavour

(1) In your current role at xxxx, as a xxxx, you do xxx (insert your job description). Can you tell us about what your job involves?

## (2) Can you share with us some complexities in managing cloud computing projects?

Contractor controls access to applications and data on cloud.

Monitoring is not easy for Thai cloud.



(3) In managing (outsourced) cloud projects, what are useful tips you could share with IT professionals to avoid common pitfalls?

As contracting office, designated officers should have at least read access to cloud resources.

## Motivation

What made you decide to earn your CCSK?

# CCSK Plus #1, November 2014

CSA Certificate of Cloud Security Knowledge Plus (CCSK) #1



Nantawan Wongkachonkitti, Ph.D.  
CIO & Deputy Manager General of Student  
Loan Funds, first CCSK passer in Thailand



# Cloud Security Alliance

Certificate of Completion Awarded to

Maykin Warasart

For Successfully Completing

## Certificate of Cloud Security Knowledge V4

Including the Following Bodies of Knowledge:

- Cloud Security Alliance - Security Guidance for Critical Areas of Focus in Cloud Computing V4
- Cloud Security Alliance - Cloud Controls Matrix
- ENISA - Cloud Computing: Benefits, Risks and Recommendations for Information Security

Jim Reavis

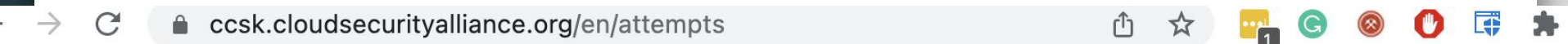
Co-founder and Chief Executive Officer, CSA



February 23, 2022

Date of Completion



# Two attempts per CCSK exam token



Exam Version	Test Started	Test Graded	Score	Status
<a href="#">CCSKv4 - English</a>	October 8, 2020 - 21:27:26	October 8, 2020 - 22:54:30	78%	 Failed
<a href="#">CCSKv4 - English</a>	May 30, 2022 - 19:37:00	May 30, 2022 - 21:06:01	93%	 Passed - <a href="#">Download (PDF)</a> - <a href="#">View Badge</a>

## Preparation

What part of the material from the CCSK has been the most relevant in your work and why?

DEPA program

KMITL

# CCSK, CCSP & vendor specific cert

What's the value in a vendor-neutral certificate like the CCSK or CCSP versus getting certified by AWS? In what scenario are the different certificates important?

Broad and general knowledge, plus overall best practices.

AWS, Azure, GCP, Alibaba, Huawei, Tencent



# Certificate vs Certification

A certificate recognizes a candidate's knowledge, skills and abilities typically as framed by a job role. A certificate scope is narrower, and only provides proof of a training course completion.

# Certificate vs Certification

A certification grants a candidate access to a membership organization, and almost always requires an annual continuing professional education (CPE) commitment to maintain the certification. But a certificate does not often associate one with any membership organization, and the body of knowledge gained does not evolve over time or require a CPE.

# CCSP

Domain 1. Cloud Concepts, Architecture and Design

Domain 2. Cloud Data Security

Domain 3. Cloud Platform and Infrastructure Security

Domain 4. Cloud Application Security

Domain 5. Cloud Security Operations

Domain 6. Legal, Risk and Compliance

# CCSK

## DOMAIN 1

**Cloud Computing  
Concepts and Architectures**



## DOMAIN 2

**Governance and Enterprise  
Risk Management**



## DOMAIN 3

**Legal Issues, Contracts and  
Electronic Discovery**



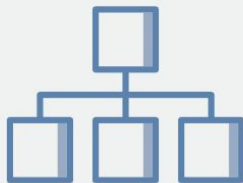
## DOMAIN 4

**Compliance and  
Audit Management**



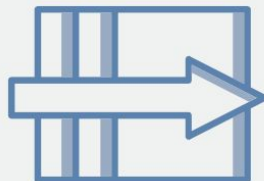
## DOMAIN 5

**Information Governance**



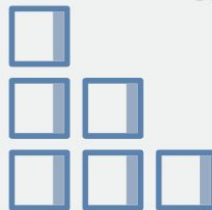
## DOMAIN 6

**Management Plane and  
Business Continuity**



## DOMAIN 7

**Infrastructure  
Security**



## DOMAIN 8

**Virtualization and Containers**



# CCSK

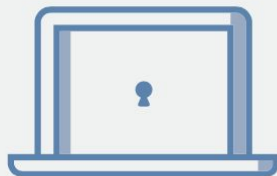
DOMAIN 9

Incident Response



DOMAIN 10

Application Security



DOMAIN 11

Data Security and Encryption



DOMAIN 12

Identity, Entitlement,  
and Access Management



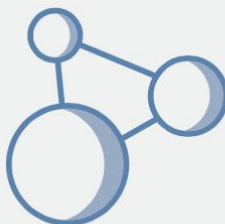
DOMAIN 13

Security as a Service



DOMAIN 14

Related Technologies



(4 / 4)

**CCM**<sup>TM</sup>

CCM

(3 / 3)



ENISA



DOMAIN 1

# Cloud Computing Concepts and Architectures



ON-DEMAND  
SELF-SERVICE



BROAD  
NETWORK  
ACCESS



RESOURCE  
POOLING



RAPID  
ELASTICITY OR  
EXPANSION



MEASURED  
SERVICE

*Essential  
Characteristics*

**SaaS**

(Software as a Service)

**PaaS**

(Platform as a Service)

**IaaS**

(Infrastructure as a Service)

*Service  
Models*

Public

Private

Hybrid

Community

*Deployment  
Models*

## Essential Characteristics:

*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 each service provider.

*Broad network access.* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

*Resource pooling.* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

*Rapid elasticity.* Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

*Measured service.* Cloud systems automatically control and optimize resource use by leveraging a metering capability<sup>1</sup> at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.



## 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 each service provider.

# Rapid elasticity

Capabilities can be elastically provisioned and released,  
in some cases automatically,  
to scale rapidly outward and inward commensurate with demand.

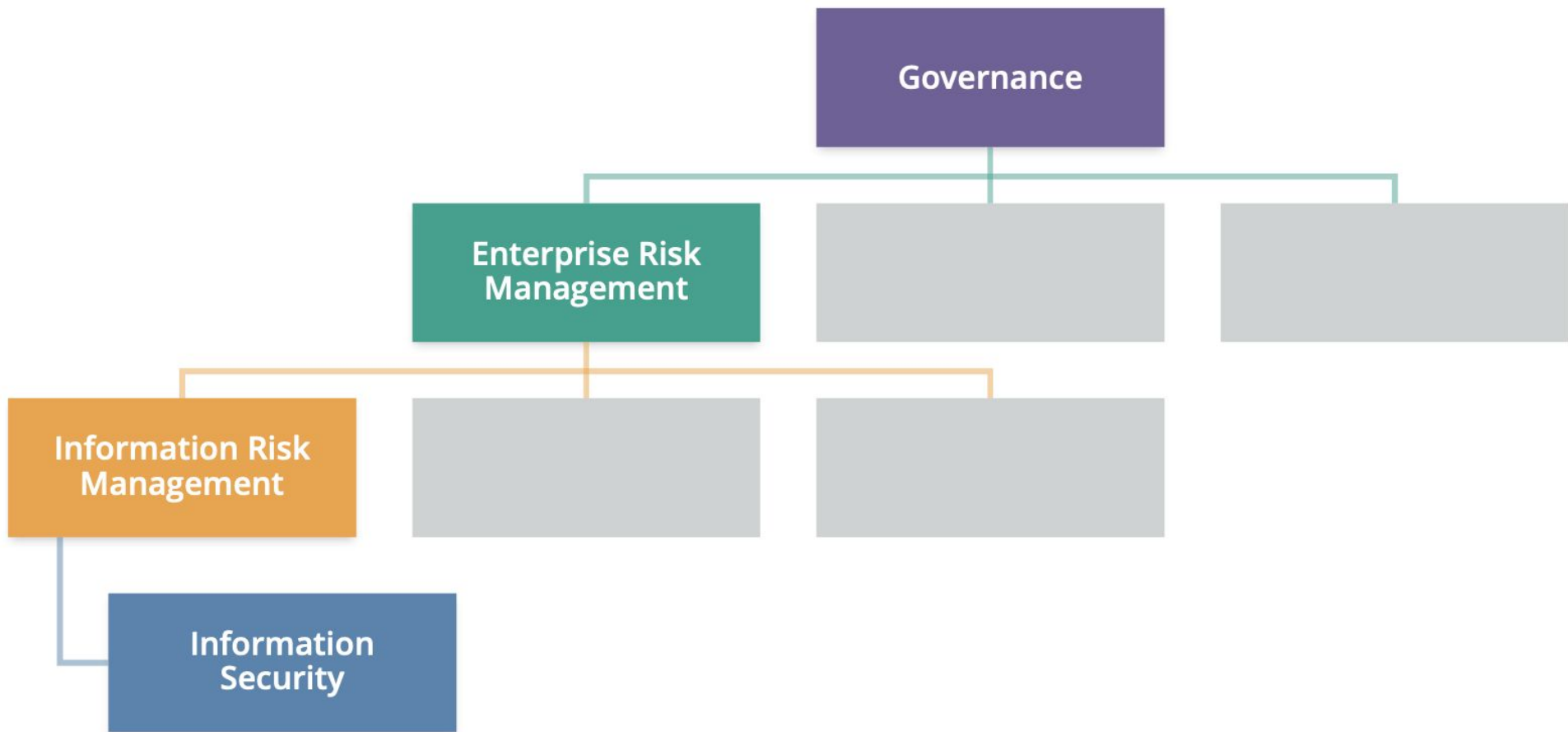
To the consumer, the capabilities available for provisioning often appear to be unlimited  
and can be appropriated in any quantity at any time.

Without essential characteristics, it can never be a “proper” cloud service, but rather a Virtual Private Server (VPS).

DOMAIN 2

# **Governance and Enterprise Risk Management**





DOMAIN 3

# **Legal Issues, Contracts and Electronic Discovery**



**Treaties**

**Contract  
jurisdiction**

**Applicable  
legislation**

**Standard  
of care**

**Location  
of services**



DOMAIN 4

# **Compliance and Audit Management**





**Compliant**  
Customer  
Application

**Non-Compliant**  
Customer  
Application

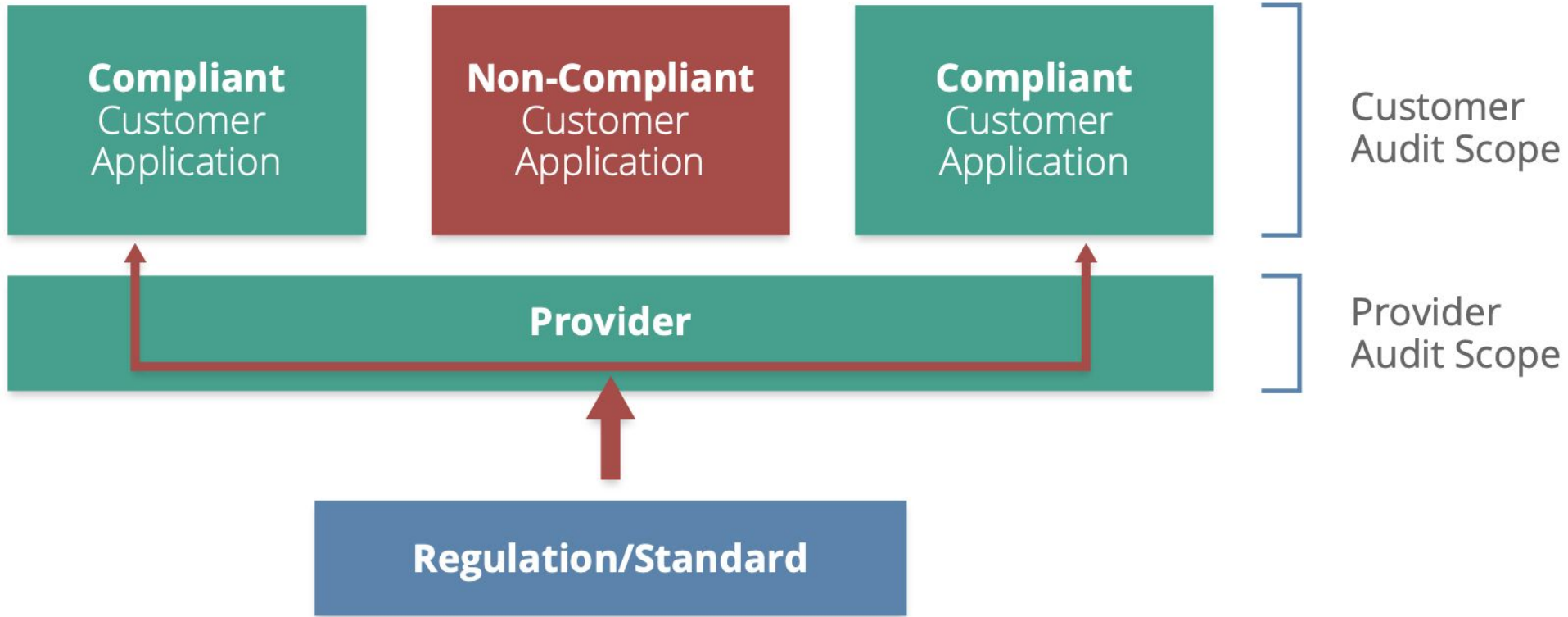
**Compliant**  
Customer  
Application

Customer  
Audit Scope

**Provider**

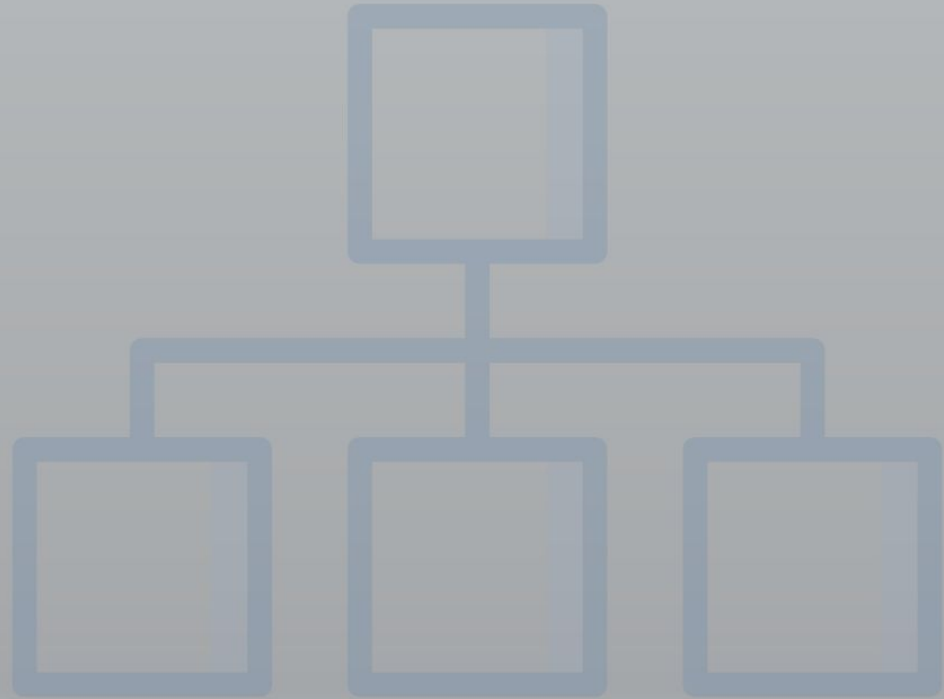
Provider  
Audit Scope

**Regulation/Standard**

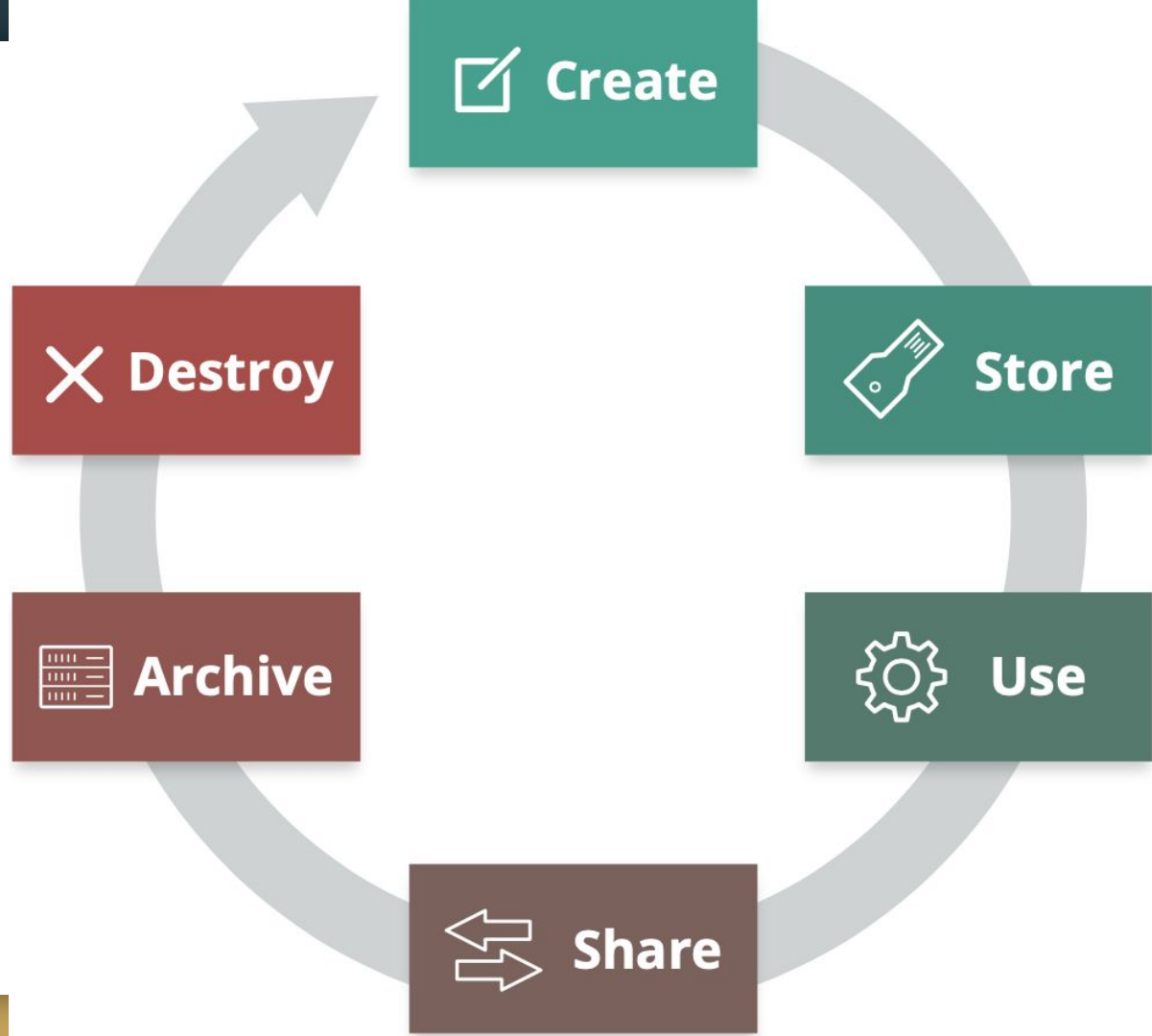


# DOMAIN 5

## **Information Governance**



# Data Security Lifecycle



DOMAIN 6

# Management Plane and Business Continuity



**Service**

**Service**

**Service**

**Service**

**Service Admin**

**Service  
Admin**

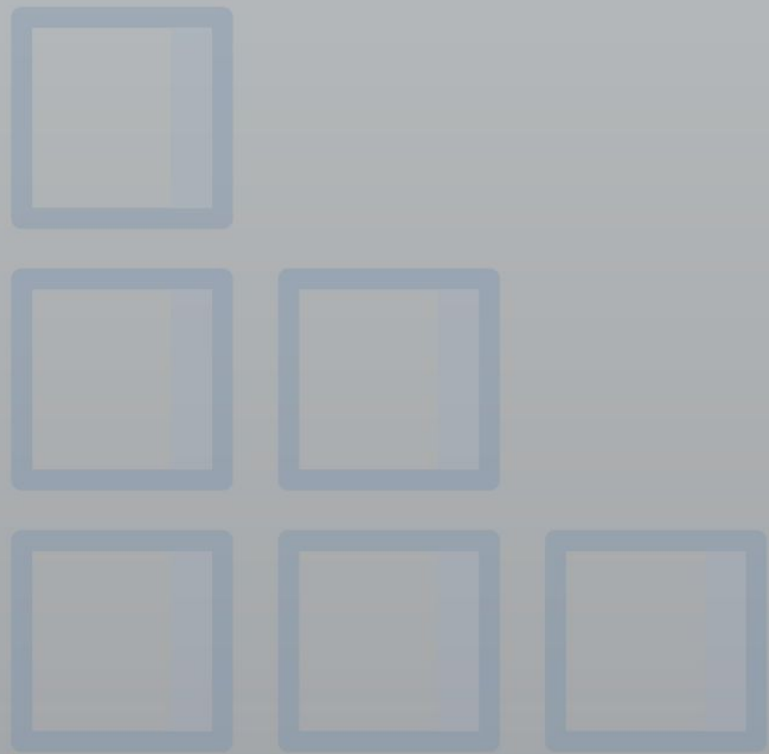
**Service  
Admin**

**Super-Admin**

**Root/Master Account**

# DOMAIN 7

## **Infrastructure Security**



# Common networks underlying IaaS

## Management

- Management plane to nodes

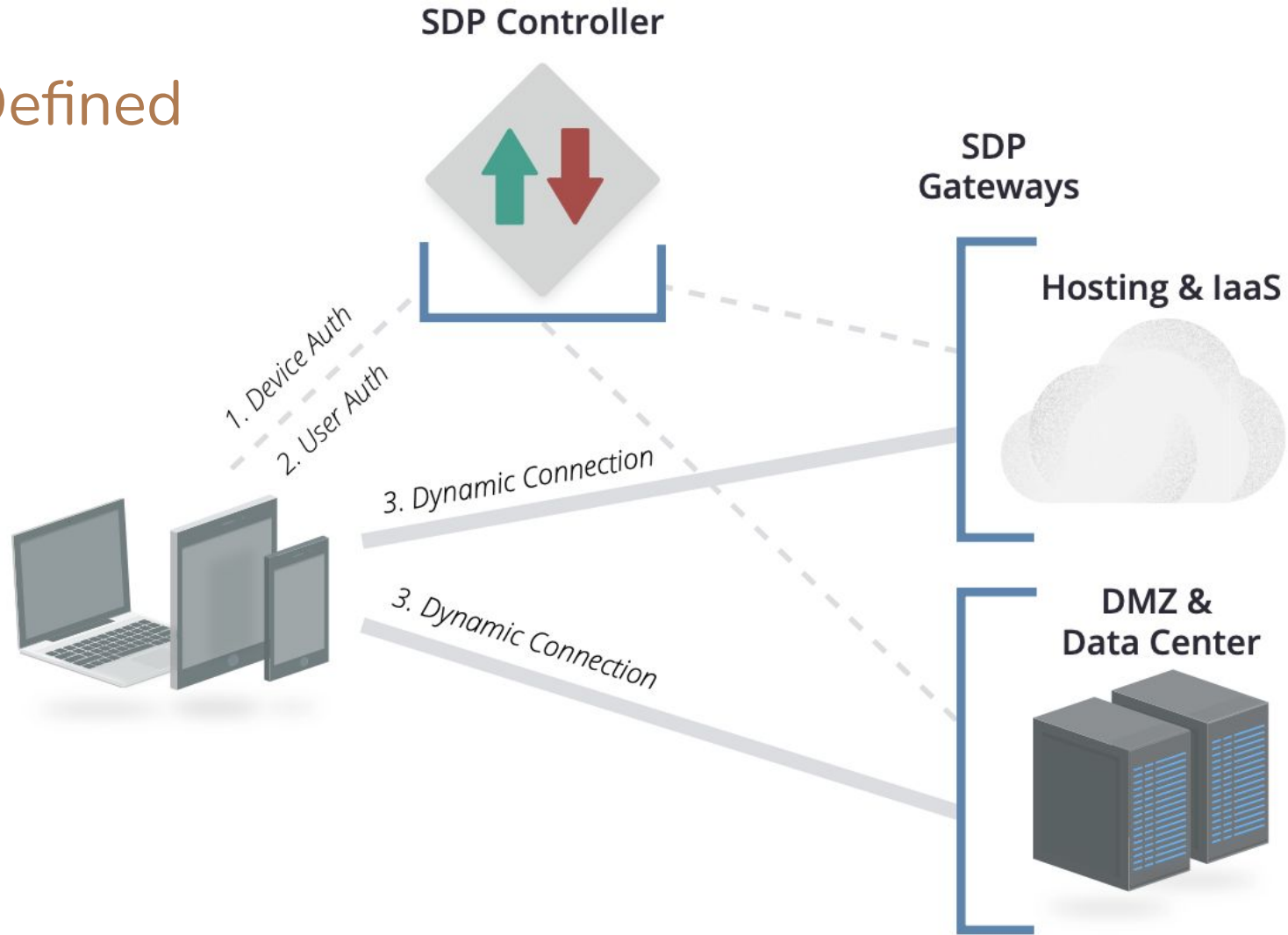
## Storage

- Storage nodes (volumes) to compute nodes (instances)

## Service

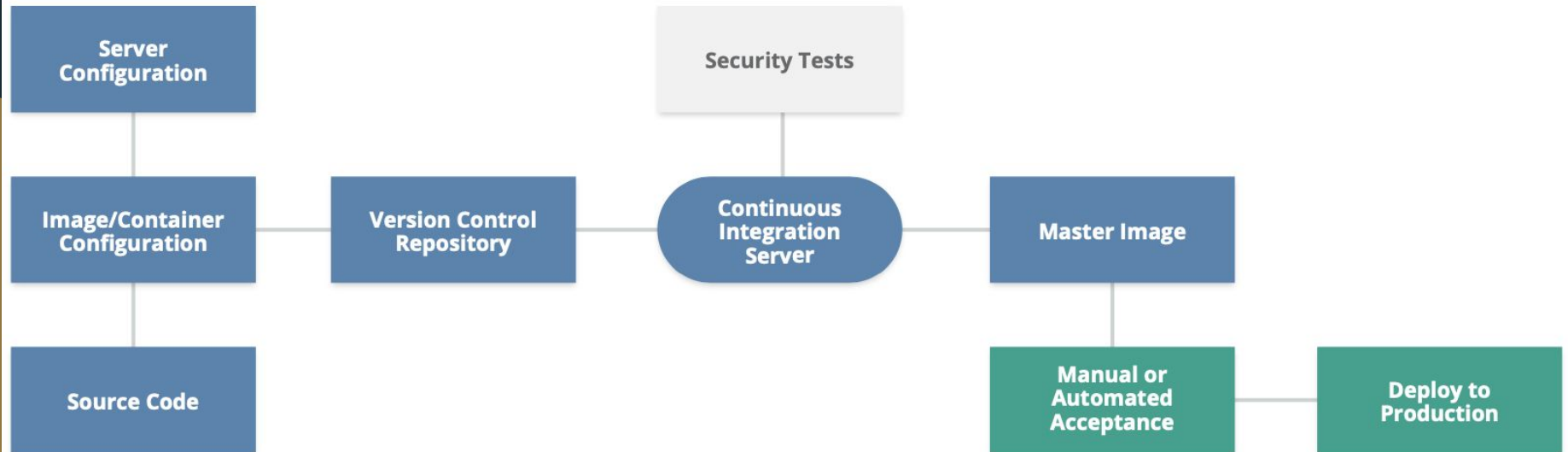
- Internet to compute nodes
- Instances to instance

# Software Defined Perimeter





deployment pipeline for creating images for immutable VMs or containers.



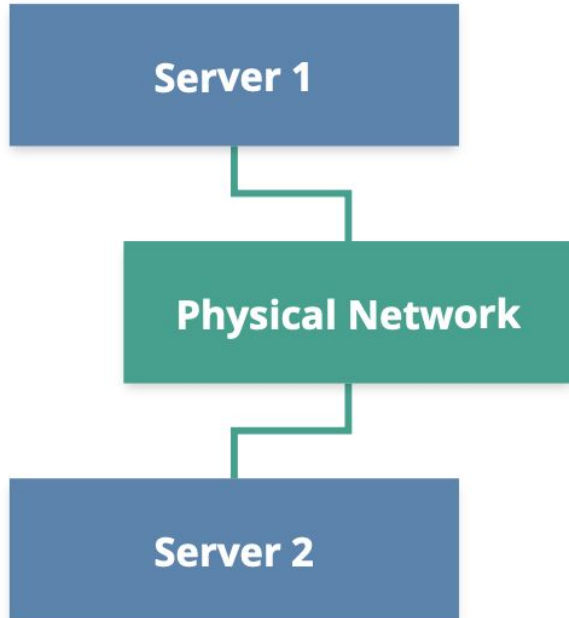
# DOMAIN 8

## **Virtualization and Containers**

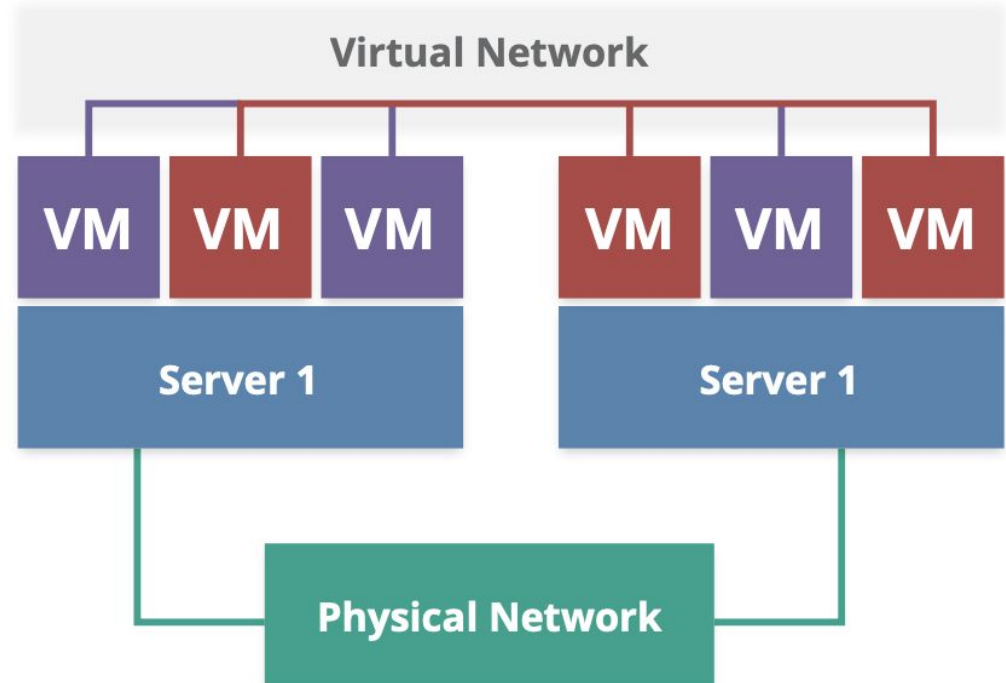


Virtual networks move packets in software and monitoring can't rely on sniffing the physical

## Before



## After



# DOMAIN 9

## **Incident Response**



# Incident Response Lifecycle

**Preparation**

**Detection  
& Analysis**

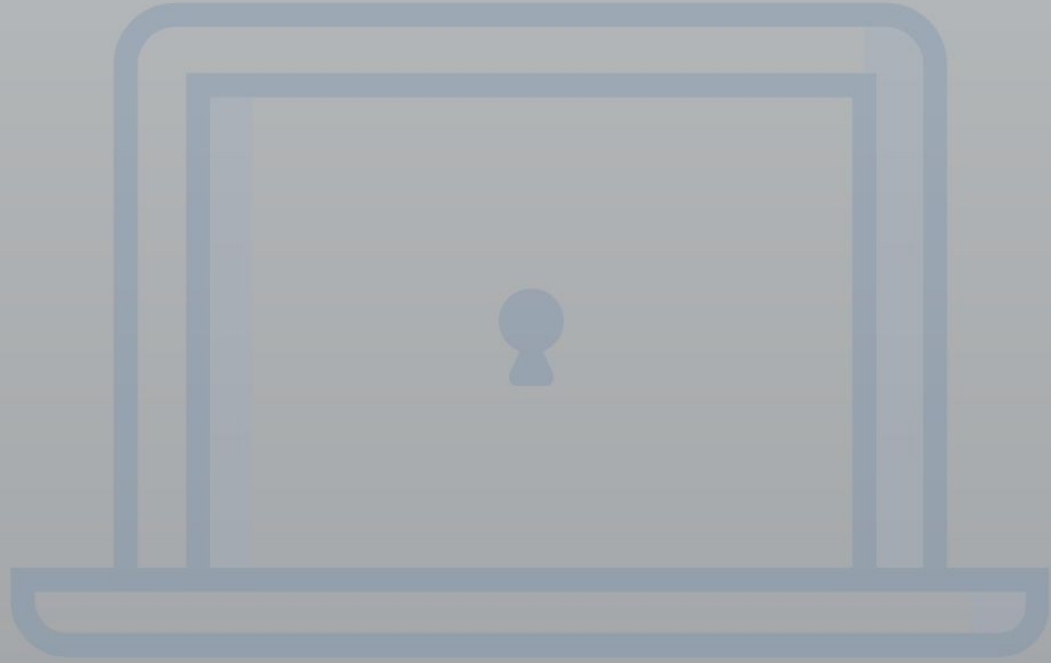
**Containment,  
Eradication,  
Recovery**

**Post-Mortem**

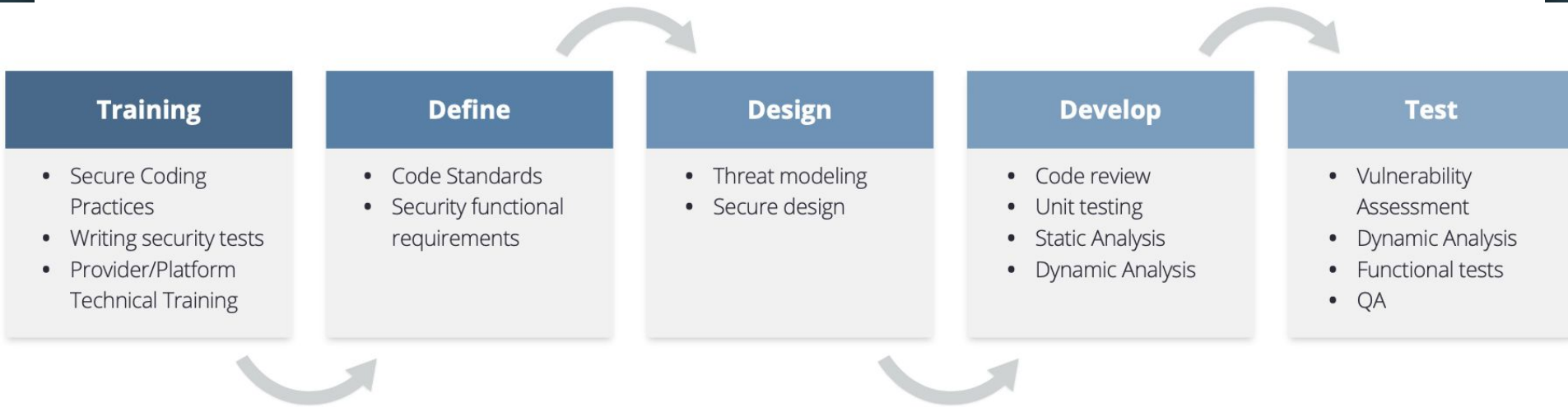


# DOMAIN 10

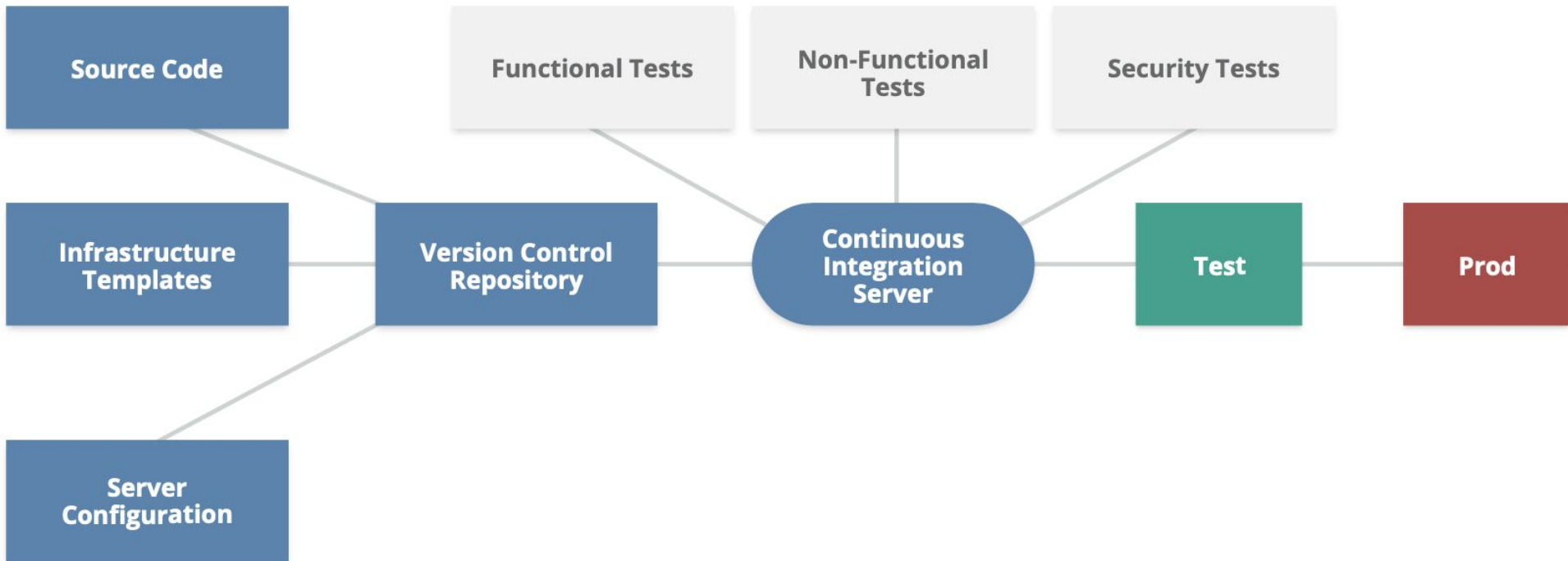
# **Application Security**



# Secure application design and development phases



# continuous deployment pipeline



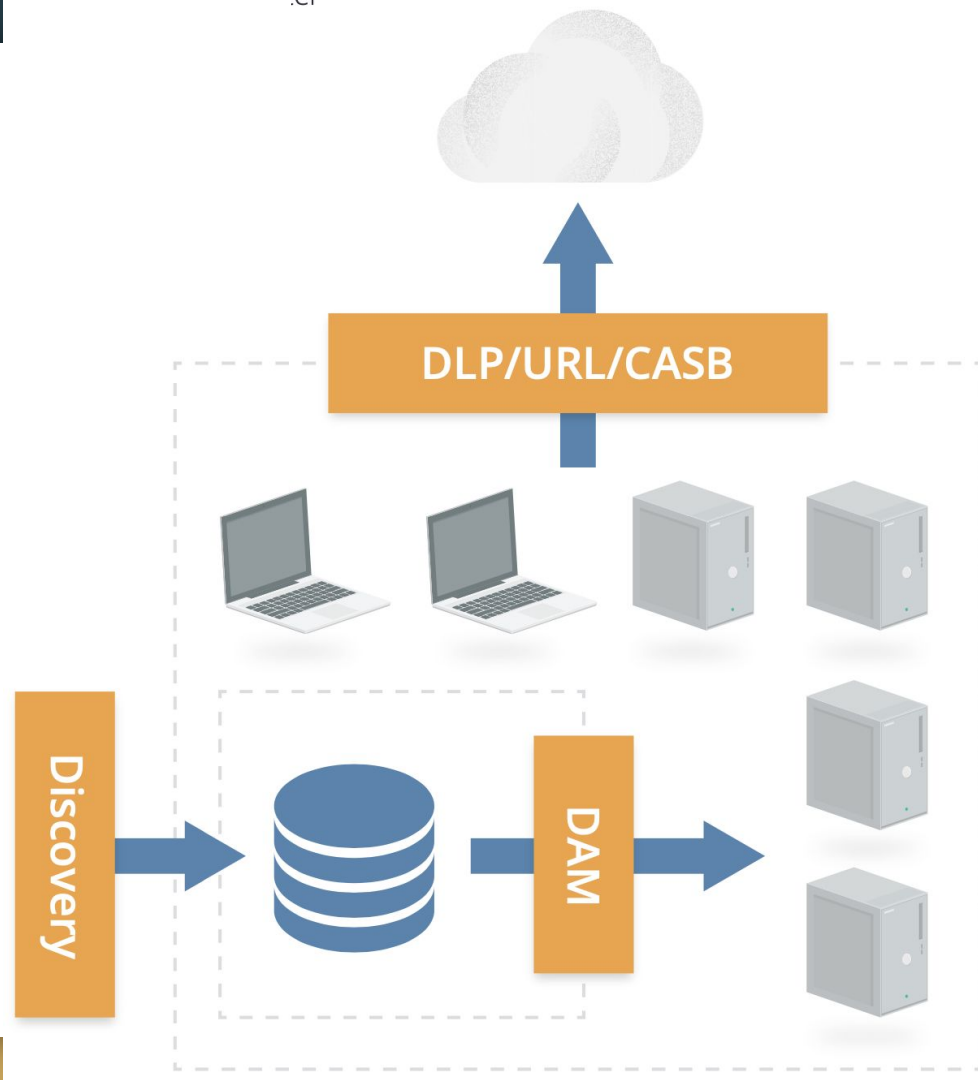


# DOMAIN 11

## **Data Security and Encryption**



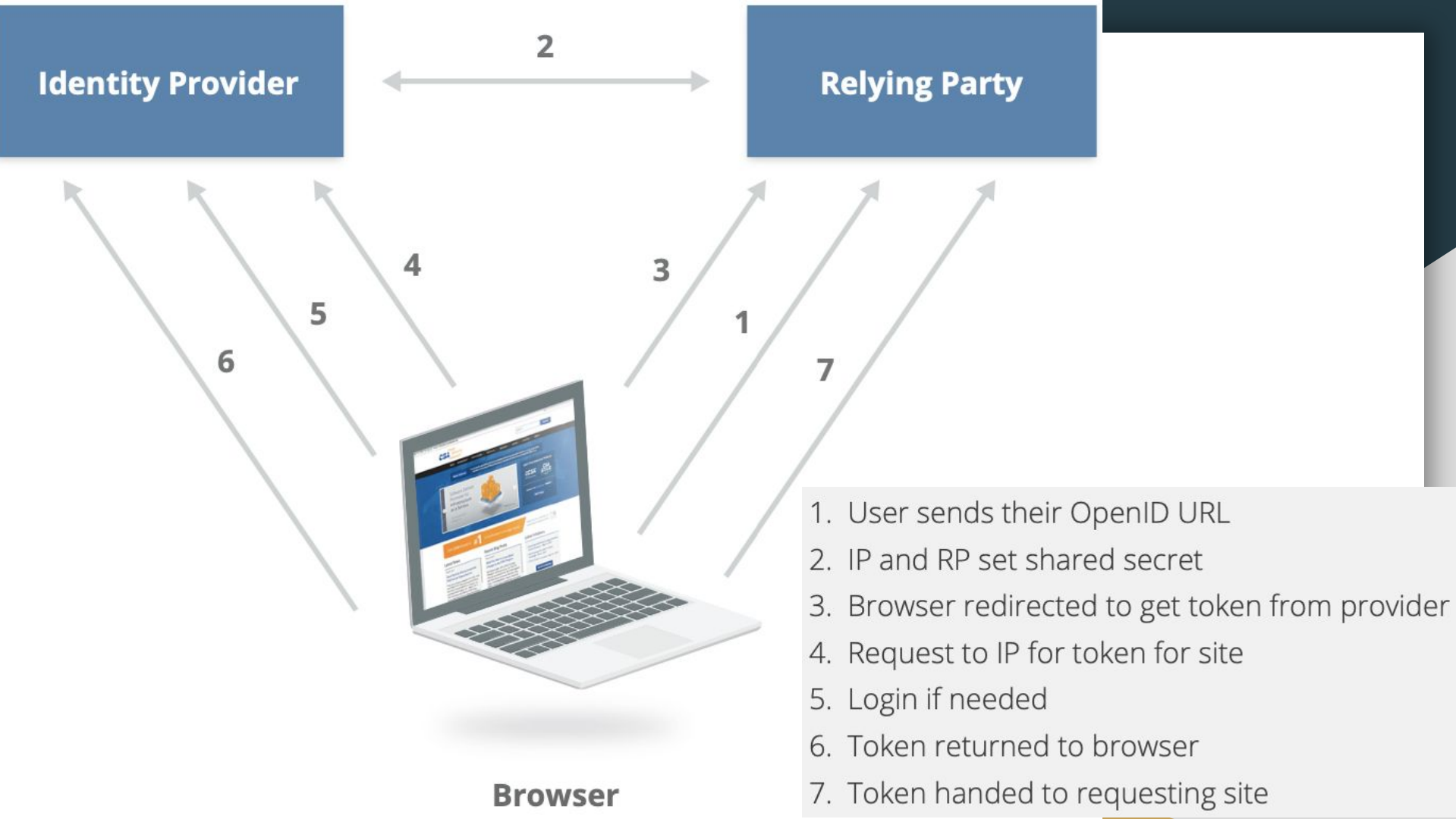
# Managing data migrations to the cloud.



DOMAIN 12

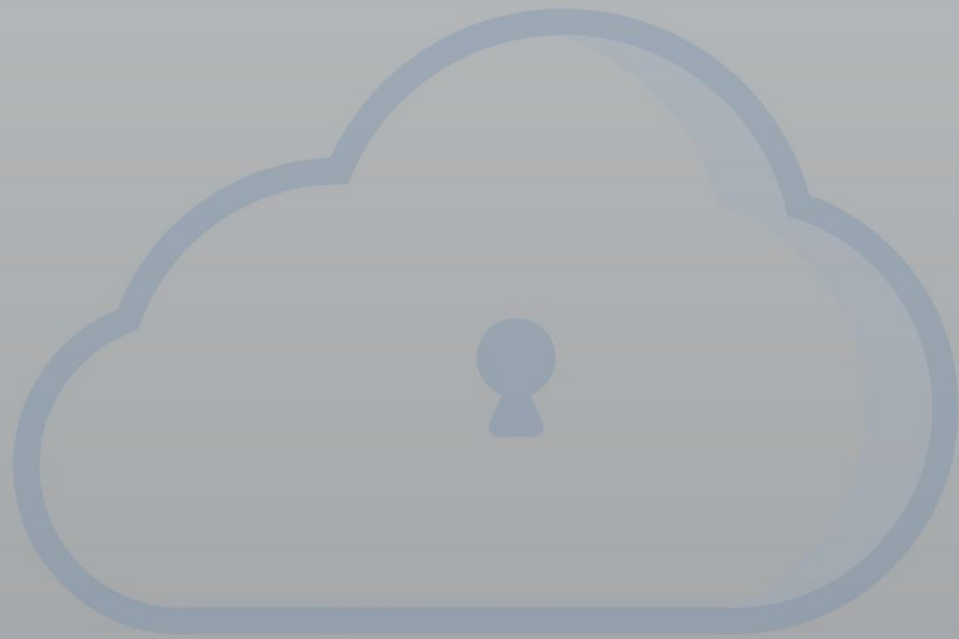
# **Identity, Entitlement, and Access Management**





# DOMAIN 13

## **Security** as a Service



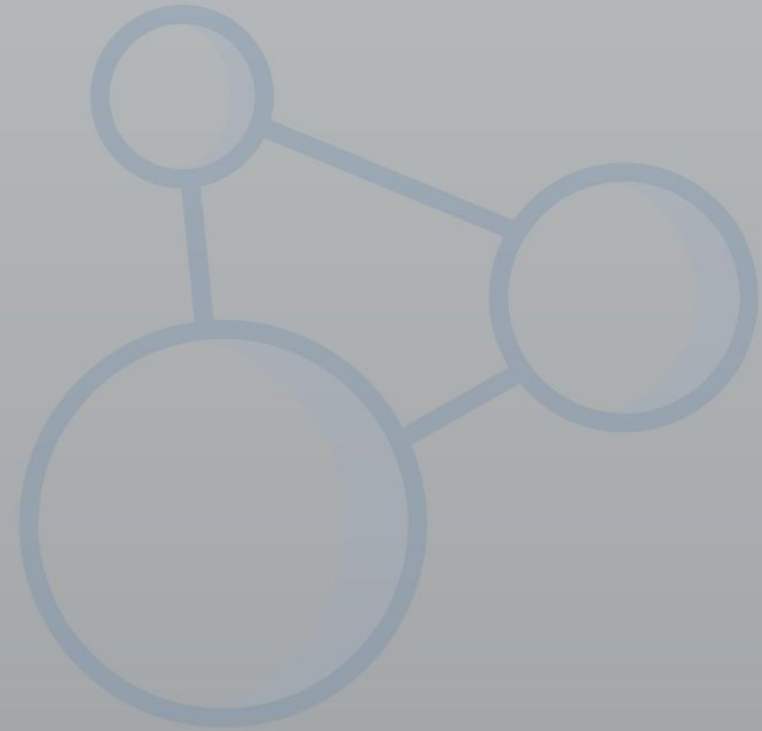
# SECaaS

<https://cloudsecurityalliance.org/research/artifacts/?term=security-as-a-service>

1. Identity and Access Management
2. Data Loss Prevention
3. Web Security
4. Email Security
5. Security Assessments
6. Intrusion Management
7. Security, Information and Event Management
8. Encryption
9. BC/DR
10. Network Security

# DOMAIN 14

## **Related Technologies**



## The current list of Related Tech includes:

- Big Data
- Internet of Things (IoT)
- Mobile devices
- Serverless computing



## (5) How does CCM help communicate with customers?

[https://downloads.cloudsecurityalliance.org/initiatives/ccm/CSA\\_CCM\\_v3.0.xlsx](https://downloads.cloudsecurityalliance.org/initiatives/ccm/CSA_CCM_v3.0.xlsx)

<https://docs.google.com/presentation/d/1qFr9Mm8jiCzfm2roGsfbTR8GaUKwudfgw-tJLYOwnfg/edit?usp=sharing>

# CCM's Control Domains

1. Application & Interface Security
2. Audit Assurance & Compliance
3. Business Continuity Management & Operational Resilience
4. Change Control & Configuration Management
5. Data Security & Information Lifecycle Management
6. Datacenter Security
7. Encryption & Key Management
8. Governance and Risk Management
9. Human Resources
10. Identity & Access Management
11. Infrastructure & Virtualization Security
12. Interoperability & Portability
13. Mobile Security
14. Security Incident Management, E-Discovery & Cloud Forensics
15. Supply Chain Management, Transparency and Accountability
16. Threat and Vulnerability Management

# Application & Interface Security

1. Application Security
2. Customer Access Requirements
3. Data Integrity
4. Data Security / Integrity

# Audit Assurance & Compliance

1. Audit Planning
2. Independent Audits
3. Information System Regulatory Mapping

# Business Continuity Management & Operational Resilience

1. Business Continuity Planning
2. Business Continuity Testing
3. Datacenter Utilities / Environmental Conditions
4. Documentation
5. Environmental Risks
6. Equipment Location
7. Equipment Maintenance
8. Equipment Power Failures
9. Impact Analysis
10. Management Program
11. Policy
12. Retention Policy

# Change Control & Configuration Management

1. New Development / Acquisition
2. Outsourced Development
3. Quality Testing
4. Unauthorized Software Installations
5. Production Changes

# Data Security & Information Lifecycle Management

1. Classification
2. Data Inventory / Flows
3. eCommerce Transactions
4. Handling / Labeling / Security Policy
5. Information Leakage
6. Non-Production Data
7. Ownership / Stewardship
8. Secure Disposal

# Datacenter Security

1. Asset Management
2. Controlled Access Points
3. Equipment Identification
4. Off-Site Authorization
5. Off-Site Equipment
6. Policy
7. Datacenter Security - Secure Area Authorization
8. Unauthorized Persons Entry
9. User Access



# Encryption & Key Management

1. Entitlement
2. Key Generation
3. Sensitive Data Protection
4. Storage and Access

# Governance and Risk Management

1. Baseline Requirements
2. Data Focus Risk Assessments
3. Management Oversight
4. Management Program
5. Management Support/Involvement
6. Policy
7. Policy Enforcement
8. Policy Impact on Risk Assessments
9. Policy Reviews
10. Risk Assessments
11. Risk Management Framework
12. Risk Mitigation / Acceptance

# Human Resources

1. Asset Returns
2. Background Screening
3. Employment Agreements
4. Employment Termination
5. Industry Knowledge / Benchmarking
6. Mobile Device Management
7. Non-Disclosure Agreements
8. Roles / Responsibilities
9. Technology Acceptable Use
10. Training / Awareness
11. User Responsibility
12. Workspace

# Identity & Access Management

1. Audit Tools Access
2. Credential Lifecycle / Provision Management
3. Diagnostic / Configuration Ports Access
4. Policies and Procedures
5. Segregation of Duties
6. Source Code Access Restriction
7. Third Party Access
8. Trusted Sources
9. User Access Authorization
10. User Access Reviews
11. User Access Revocation
12. User ID Credentials
13. Utility Programs Access

# Infrastructure & Virtualization Security

1. Audit Logging / Intrusion Detection
2. Change Detection
3. Clock Synchronization
4. Information System Documentation
5. Management - Vulnerability Management
6. Network Security
7. OS Hardening and Base Controls
8. Production / Non-Production Environments
9. Segmentation
10. VM Security - vMotion Data Protection
11. VMM Security - Hypervisor Hardening
12. Wireless Security

# Interoperability & Portability

1. APIs
2. Data Request
3. Policy & Legal
4. Standardized Network Protocols
5. Virtualization

# Mobile Security

1. Anti-Malware
2. Application Stores
3. Approved Applications
4. Approved Software for BYOD
5. Awareness and Training
6. Cloud Based Services
7. Compatibility
8. Device Eligibility
9. Device Inventory
10. Device Management
11. Encryption
12. Jailbreaking and Rooting
13. Legal
14. Lockout Screen
15. Operating Systems
16. Passwords
17. Policy
18. Remote Wipe
19. Security Patches
20. Users

# Security Incident Management, E-Discovery & Cloud Forensics

1. Contact / Authority Maintenance
2. Incident Management
3. Incident Reporting
4. Incident Response Legal Preparation
5. Incident Response Metrics



# Supply Chain Management, Transparency and Accountability

1. Data Quality and Integrity
2. Incident Reporting
3. Network / Infrastructure Services
4. Provider Internal Assessments
5. Supply Chain Agreements
6. Supply Chain Governance Reviews
7. Supply Chain Metrics
8. Third Party Assessment
9. Third Party Audits

# Threat and Vulnerability Management

1. Anti-Virus / Malicious Software
2. Vulnerability / Patch Management
3. Mobile Code

# Scope Applicability

1. AICPA, TS Map
2. AICPA, Trust Service Criteria (SOC 2SM Report)
3. BITS Shared Assessments, AUP v5.0
4. BITS Shared Assessments, SIG v6.0
5. BSI Germany
6. CCM V1.X
7. COBIT 4.1
8. CSA Enterprise Architecture / Trust Cloud Initiative
9. CSA Guidance V3.0
10. ENISA IAF
11. FedRAMP Security Controls (Final Release, Jan 2012)  
--LOW IMPACT LEVEL--
12. FedRAMP Security Controls (Final Release, Jan 2012)  
--MODERATE IMPACT LEVEL--
13. GAPP (Aug 2009)
14. HIPAA / HITECH Act
15. ISO/IEC 27001-2005
16. Jericho Forum
17. NERC CIP
18. NIST SP800-53 R3
19. NZISM
20. PCI DSS v2.0

# ENISA's Cloud Computing Risk Assessment

European Network and Information  
Security Agency

European Union Agency for Cybersecurity

<https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment>

1. Security benefits of cloud computing
2. Risk assessment
3. Risks
  - 3.1 Policy and organizational risks
  - 3.2 Technical risks
  - 3.3 Legal risks
  - 3.4 Risks not specific to the cloud
4. Vulnerabilities
5. Assets
6. Recommendations and key messages
  - 6.1 Information assurance framework
  - 6.2 Informational assurance requirements
  - 6.3 Research recommendations, e.g. trust in the cloud, data protection, large-scale systems engineering

(7) Would you encourage your staff and/or colleagues to obtain CCSK or other CSA qualifications? Why?

CCSK then CCAK to understand how to assess proper cloud services.

## (8) What is the best advice you will give to IT professionals in order for them to scale new heights in their careers?

In organizations that can never keep up with ever expanding IT resources, cloud is a must.

Knowing how to manage cloud resources and maintain reliable & resilient cloud operations, one needs proper cloud certification.