iiNURTURE
Education Solutions
TOMORROW'S HERE

Cloud Security

Module Number: 04

Module Name: Cloud Security Controls

Version Code:CS1
Released Date:20-Feb-2019

Cloud Security Controls

AIM:

To equip the students with security and control measures of cloud architecture.

Cloud Security Controls

Objectives:

The Objectives of this module are:

- Define the architecture of cloud.
- List the architecture and reference model of Trusted Cloud Initiative.
- Utility of CCM in Cloud security and its application.

Cloud Security Controls

Outcomes:

At the end of this module, you are expected to:

- Explain TCI architecture.
- Outline different domains of TCI.

Cloud Security Controls

Contents

- Concept of Cloud Control Matrix
- TCI Architecture
- Domain of Cloud Control Matrix
- Mapping Cloud Controls

Cloud Security Controls

Cloud control Matrix

- Cloud Controls Matrix (CCM) is specially designed to deliver important security principles to guide cloud server providers and to assist potential cloud customers in evaluating overall security risk of cloud service provider.
- It provides a controlled framework for thorough understanding of security concepts and values that are associated to the Cloud Security Alliance guidelines in 13 various domains.
- The fundamentals of the Cloud Security Matrix rest on its customized relationship to other industry security standards, & control frameworks such as the ISO 27001 / 27002, ISACA- COBIT, NIST, and PCI.

Cloud Security Controls

Cloud control Matrix

- The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.
- Data governance domain of Cloud Control Matrix will manage all the possible situations of data misuse, misuse, leakage of information, disposal of data, custody and related risks.

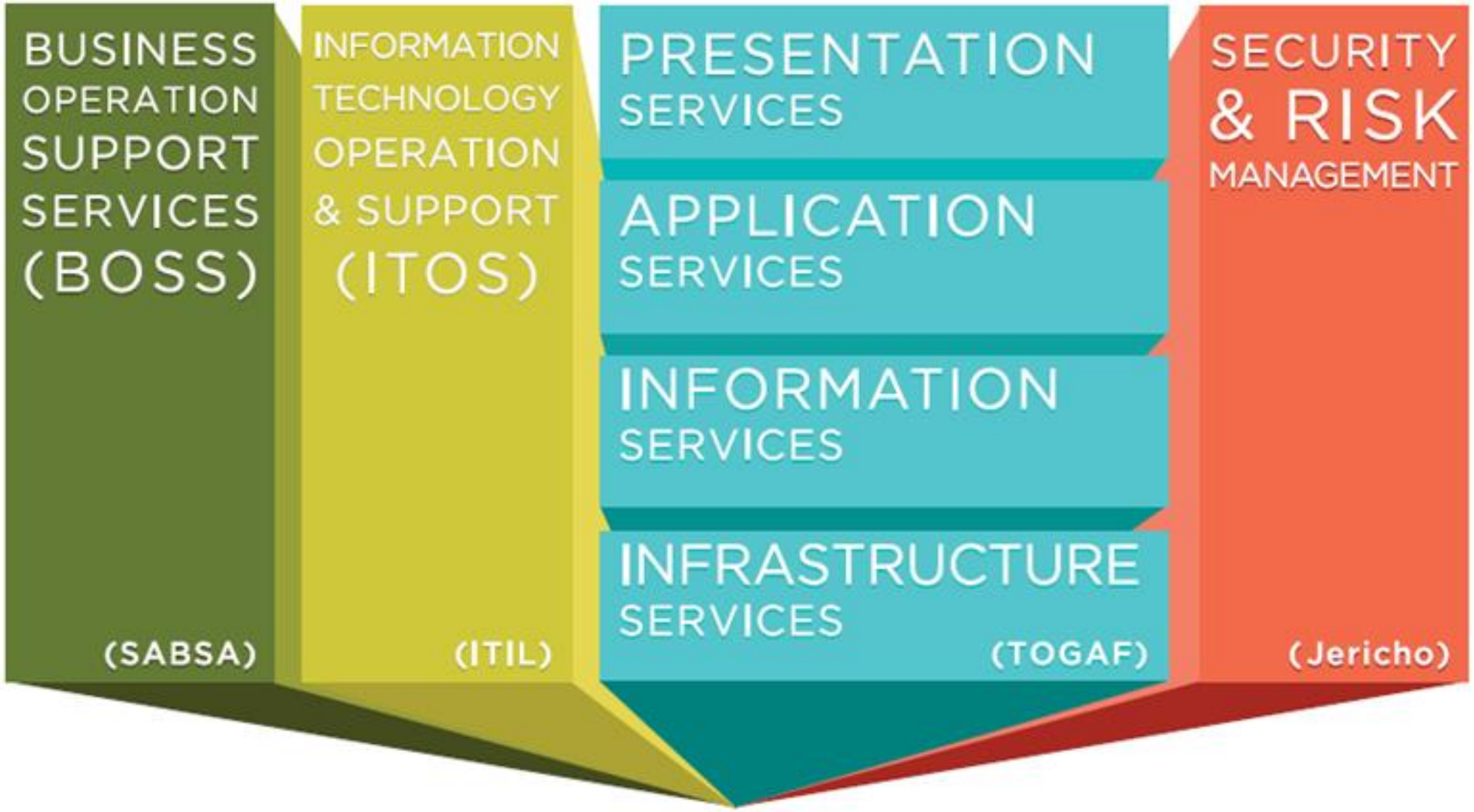
Cloud Security Controls

TCI architecture is having both methodology and the set of tools

Cloud Security Controls

- Enable security architects, enterprise architects, and risk management professional to influence a common set of solutions.
- These solutions accomplish a set of common requirements that risk managers must access the operational status of internal IT security and cloud provider control.
- These various controls are conveyed in terms of security capabilities and designed to create a common map to meet the security needs of their business.

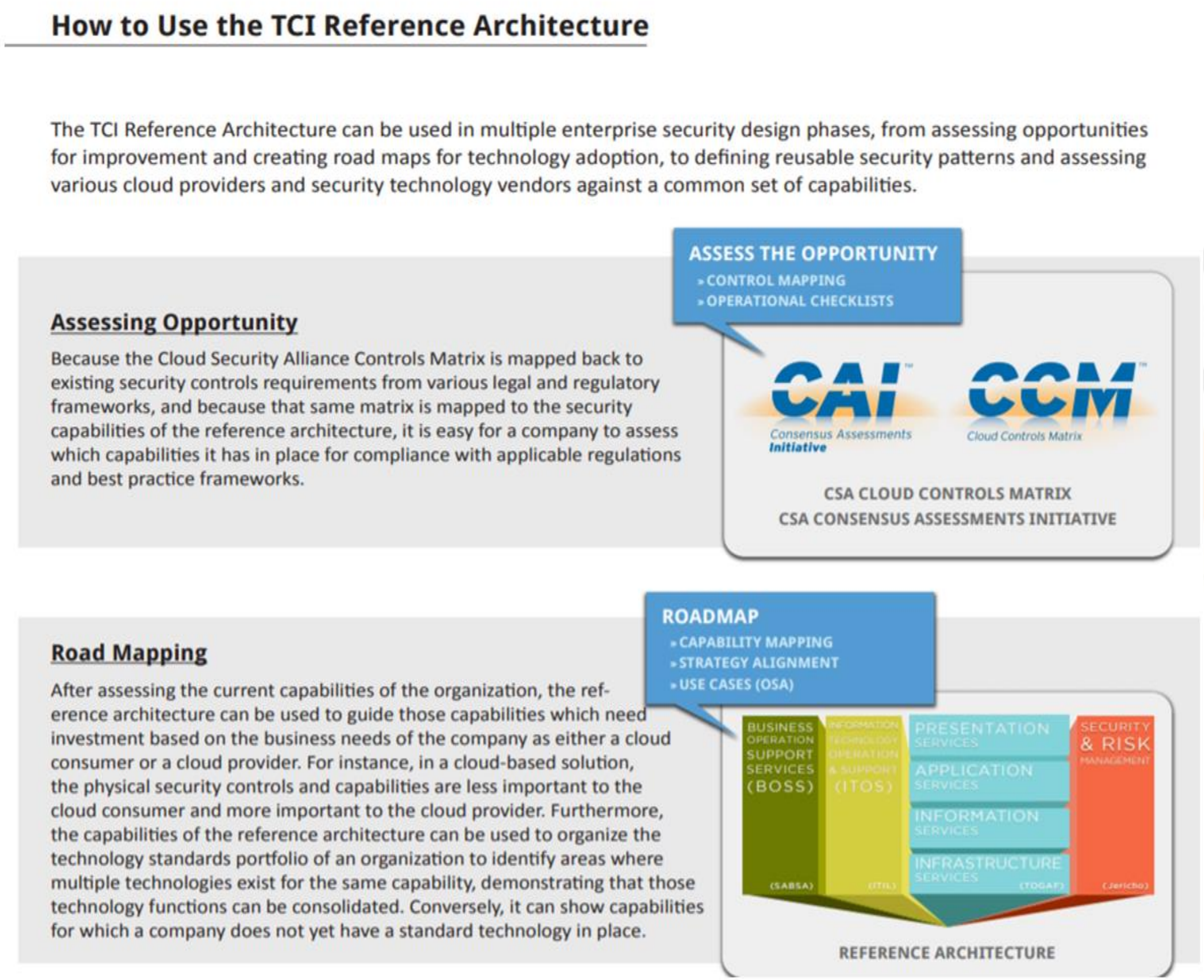
Cloud Security Controls


BUSINESS OPERATION SUPPORT SERVICES (BOSS)
(SABSA)
INFORMATION TECHNOLOGY OPERATION & SUPPORT (ITOS)
(ITIL)
PRESENTATION SERVICES
APPLICATION SERVICES
INFORMATION SERVICES
INFRASTRUCTURE SERVICES
(TOGAF)
SECURITY & RISK MANAGEMENT
(Jericho)

cloud

TCI Reference Architecture

Cloud Security Controls



How to Use the TCI Reference Architecture

The TCI Reference Architecture can be used in multiple enterprise security design phases, from assessing opportunities for improvement and creating road maps for technology adoption, to defining reusable security patterns and assessing various cloud providers and security technology vendors against a common set of capabilities.

Assessing Opportunity

Because the Cloud Security Alliance Controls Matrix is mapped back to existing security controls requirements from various legal and regulatory frameworks, and because that same matrix is mapped to the security capabilities of the reference architecture, it is easy for a company to assess which capabilities it has in place for compliance with applicable regulations and best practice frameworks.

ASSESS THE OPPORTUNITY
- » CONTROL MAPPING
- » OPERATIONAL CHECKLISTS

CSA CLOUD CONTROLS MATRIX
CSA CONSENSUS ASSESSMENTS INITIATIVE

Road Mapping

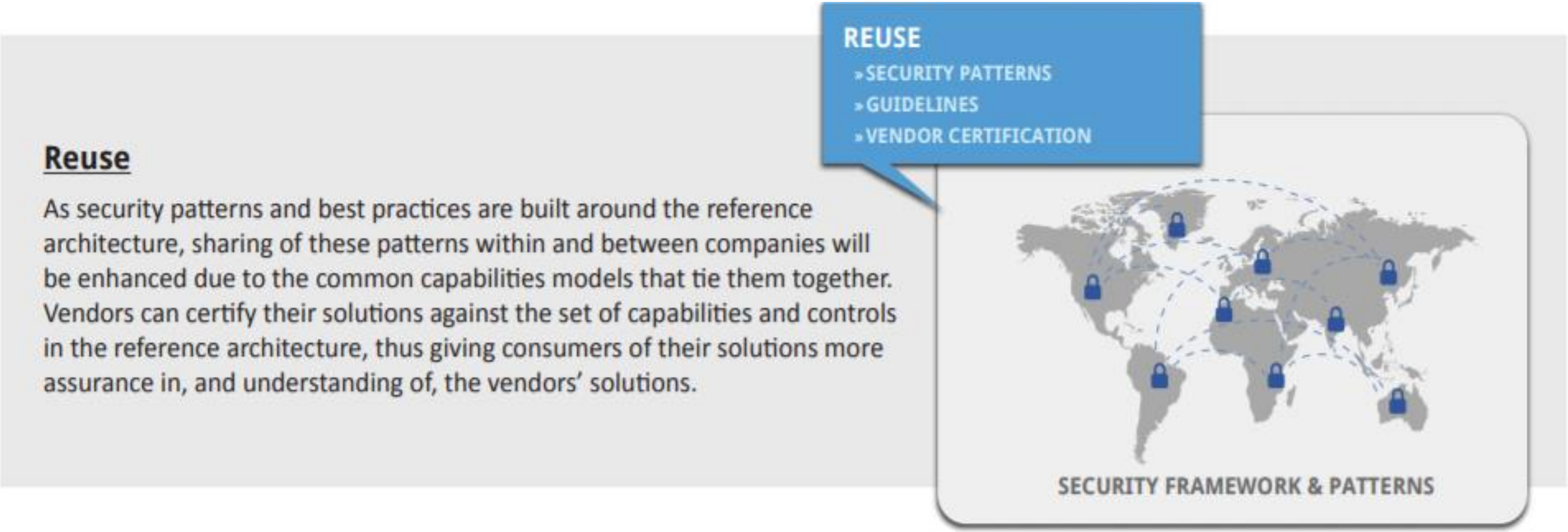
After assessing the current capabilities of the organization, the reference architecture can be used to guide those capabilities which need investment based on the business needs of the company as either a cloud consumer or a cloud provider. For instance, in a cloud-based solution, the physical security controls and capabilities are less important to the cloud consumer and more important to the cloud provider. Furthermore, the capabilities of the reference architecture can be used to organize the technology standards portfolio of an organization to identify areas where multiple technologies exist for the same capability, demonstrating that those technology functions can be consolidated. Conversely, it can show capabilities for which a company does not yet have a standard technology in place.

ROADMAP
- » CAPABILITY MAPPING
- » STRATEGY ALIGNMENT
- » USE CASES (OSA)

BUSINESS OPERATION SUPPORT SERVICES (BOSS)
(SABSA)
INFORMATION TECHNOLOGY OPERATION & SUPPORT (ITOS)
(ITIL)
PRESENTATION SERVICES
APPLICATION SERVICES
INFORMATION SERVICES
INFRASTRUCTURE SERVICES
(TOGAF)
SECURITY & RISK MANAGEMENT
(Jericho)

REFERENCE ARCHITECTURE

Cloud Security Controls



Reuse

As security patterns and best practices are built around the reference architecture, sharing of these patterns within and between companies will be enhanced due to the common capabilities models that tie them together. Vendors can certify their solutions against the set of capabilities and controls in the reference architecture, thus giving consumers of their solutions more assurance in, and understanding of, the vendors’ solutions.

REUSE

» SECURITY PATTERNS

» GUIDELINES

» VENDOR CERTIFICATION

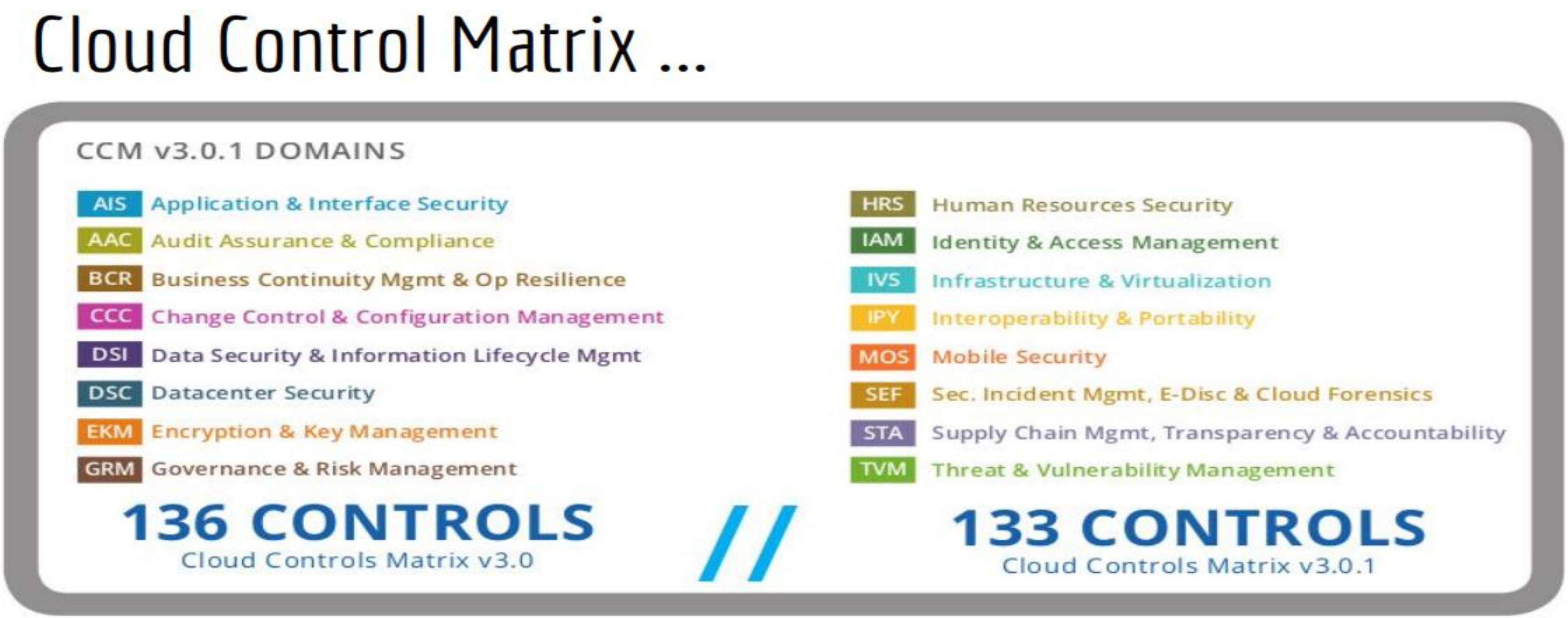
SECURITY FRAMEWORK & PATTERNS

Cloud Security Controls

Services Provided

- Governance Risk and compliance
- Information Security management
- Privilege Management Infrastructure
- Threat and Vulnerability management
- Infrastructure Protection services
- Data Protection
- Policies and standards
- Relationships with other domains

Cloud Security Controls



Cloud Control Matrix …

CCM v3.0.1 DOMAINS

AIS	Application & Interface Security
AAC	Audit Assurance & Compliance
BCR	Business Continuity Mgmt & Op Resilience
CCC	Change Control & Configuration Management
DSI	Data Security & Information Lifecycle Mgmt
DSC	Datacenter Security
EKM	Encryption & Key Management
GRM	Governance & Risk Management
HRS	Human Resources Security
IAM	Identity & Access Management
IVS	Infrastructure & Virtualization
IPY	Interoperability & Portability
MOS	Mobile Security
SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA	Supply Chain Mgmt, Transparency & Accountability
TVM	Threat & Vulnerability Management

136 CONTROLS
Cloud Controls Matrix v3.0

//

133 CONTROLS
Cloud Controls Matrix v3.0.1

Cloud Security Controls

Application and Interface Security

- Application Security- Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (**Example**., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.

- Customer Access Requirements- Prior to granting customers access to data, assets, and information systems, all identified security, contractual, and regulatory requirements for customer access shall be addressed and remediated.

- Data Integrity- Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.

Cloud Security Controls

Audit Assurance and compliance

- Audit Planning- Audit plans, activities, and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimise the risk of business process disruption.

- Independent Audits- Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure that the organisation addresses any nonconformities of established policies, procedures, and known contractual, statutory, or regulatory compliance obligations.

- Information System Regulatory Mapping- An inventory of the organization's external legal, statutory, and regulatory compliance obligations associated with any scope and geographically-relevant presence of data or organizationally-owned or managed infrastructure network and systems components shall be maintained and regularly updated as per the business need.

Cloud Security Controls

Business Continuity Management and Operational Resilience

- Business Continuity Planning- Requirements for business continuity plans include the following: Defined purpose and scope, aligned with relevant dependencies, Accessible to and understood by those who will use them, Owned by a named person who is responsible for their review, update, and approval.

- Business Continuity Testing- Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organisational or environmental changes.

- Datacentre Utilities- Datacentre utility services and environmental conditions shall be secured, monitored, maintained, and tested at planned intervals to ensure protection from unauthorised interception or damage, and designed with automated fail-over.

- Documentation- Information system documentation shall be made available to authorized personnel to ensure the following: Configuring, installing, and operating the information system, Effectively using the system’s security features

Cloud Security Controls

Business Continuity Management and Operational Resilience

- Environmental Risks- Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, solar-induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, designed, and have countermeasures applied.

Cloud Security Controls

Change Control and Configuration Management

- Acquisition- Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development of new data.

- Outsourced Development- The use of an outsourced workforce or external business relationship for designing, developing, testing, and/or deploying the organization's own source code shall require higher levels of assurance of trustworthy applications.

- Quality Testing- A program for the systematic monitoring and evaluation to ensure that standards of quality and security baselines are being met shall be established for all software developed by the organization.

- Unauthorised Software Installations- Policies and procedures shall be established and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software.

Cloud Security Controls

Change Control and Configuration Management

- Production Changes- Policies and procedures shall be established, and supporting IT governance and service management-related business processes implemented, for managing the risks associated with applying changes to business-critical or customer impacting application and system-system interface (API) designs and configurations, as well as an infrastructure network and systems components.

Cloud Security Controls

Data Security and Information Lifecycle Management

- Classification- Data and objects containing data shall be assigned a classification based on data type, criticality to the organisation, third-party obligation for retention, and prevention of unauthorized disclosure or misuse.

- E-Commerce Transactions- Data related to electronic commerce that traverses public networks shall be appropriately classified and protected from fraudulent activity or modification in such a manner to prevent contract dispute.

- Security Policy- Policies and procedures shall be established for labelling, handling, and the security of data and objects which contain data.

- Information Leakage- Security mechanisms shall be implemented to prevent data leakage.

- Ownership- All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.

Cloud Security Controls

Data centre Security

- Asset Management- Assets must be classified in terms of business criticality in support of dynamic and distributed physical and virtual computing environments, service-level expectations, and operational continuity requirements.

- Controlled Access Points- Physical security perimeters shall be implemented to safeguard sensitive data and information systems.

- Identification- Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.

- Off-Site Authorisation- Authorisation must be obtained prior to relocation or transfer of hardware, software, or data to offsite premises.

Cloud Security Controls

Encryption and Key Management

- Entitlement- All entitlement decisions shall be derived from the identities of the entities
- Key Generation- Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the management of cryptographic keys in the service's cryptosystem.
- Sensitive Data Protection- Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage.
- Storage and Access- Strong encryption in open formats and standard algorithms shall be required.

Cloud Security Controls

Governance and Risk Management

- Management Oversight- Managers are responsible for maintaining awareness of, and complying with, security policies, procedures and standards that are relevant to their area of responsibility.

- Management Programme- An Information Security Management Program shall be developed, documented, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, unauthorised access, disclosure, alteration, and destruction.

- Policy- Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships.

- Policy Enforcement- A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures.

- Policy Impact on Risk Assessment- Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.

Cloud Security Controls

Human Resources

- Asset Returns- Upon termination of workforce personnel and expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.
- Background Screening- Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification.
- Employment Termination- Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.
- Industry Knowledge- Industry security knowledge and benchmarking through networking, specialist security forums and professional associations shall be maintained.
- Mobile Device Management- Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources.

Cloud Security Controls

Identity and Access Management

- Audit Tools Access- Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.

- Diagnostic- User access to diagnostic and configuration ports shall be restricted to authorised individuals and applications.

- Policies and Procedures- Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access.

- Segregation of Duties- User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.

- Policies and Procedures- Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access.

Cloud Security Controls

Identity and Access Management

- Segregation of Duties- User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.

Cloud Security Controls

Infrastructure and Virtualization Security

- Audit Logging- Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs to support forensic investigative capabilities in the event of a security breach.

- Change Detection- The provider shall ensure the integrity of all virtual machine images at all times.

- Clock Synchronisation- A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.

- Information System Documentation- The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance.

- Network Security- Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections, reviewed at planned intervals, supported by the documented business justification for use of all services, protocols, and ports allowed, including rationale or compensating controls implemented for those protocols considered to be insecure.

Cloud Security Controls

Interoperability and Portability

- APIs- The provider shall use open and published APIs to ensure the broadest support for interoperability between components and to facilitate migrating applications.

- Data Request- All unstructured data shall be available to the customer and provided to them upon request in an industry-standard format.

- Policy and Legal- Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer requirements for service-to-service application and portability for application development and information exchange.

- Standardised Network Protocols- The provider shall use secure standardised network protocols for the import and export of data and manage the service, and shall make available a document to consumers detailing the relevant interoperability and portability standards that are involved.

Cloud Security Controls

Mobile Security

- Anti-Malware- Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.

- Application Stores- The company shall have a documented and communicated list of approved application stores that have been identified as acceptable for mobile devices accessing or storing company data and company systems.

- Approved Applications- The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.

- Approved Software for BYOD- The BYOD policy and supporting awareness training shall clearly state the approved applications and application stores that may be used for BYOD usage.

- Compatibility- The company shall have a documented application validation process to test for the device, operating system, and application compatibility issues.

Cloud Security Controls

Security Incident Management, E-Discovery and Cloud Forensics

- Authority Maintenance- Points of contact for applicable regulatory authorities and other legal jurisdictional authorities shall be maintained and regularly updated to ensure direct compliance liaisons have been established.

- Incident Management- Policies and procedures shall be established and supporting business processes and technical measures implemented, to triage security-related events and ensure.

- Incident Reporting- Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner.

- Incident Response Metrics- Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.

Cloud Security Controls

Supply Chain Management, Transparency and Accountability

- Data Quality and Integrity- Providers shall inspect, account for, and correct data quality errors and risks inherited from partners within their cloud supply-chain.

- Incident Reporting- The provider shall make security incident information available to all affected customers and providers periodically through electronic methods.

- Network Services- Business-critical or customer impacting application and system-system interface designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service.

- Provider Internal Assessments- The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.

- Supply Chain Governance Reviews- Providers shall review the risk management and governance processes of their partners to ensure that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.

Cloud Security Controls

Threat and Vulnerability Management

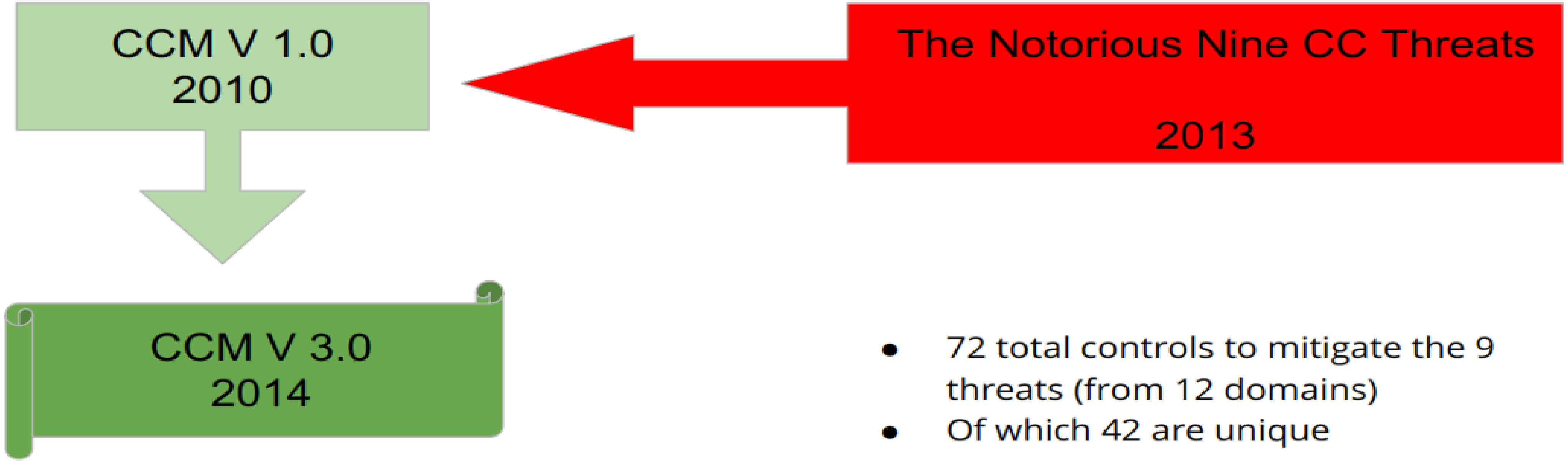
- Malicious Software- Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organisationally-owned or managed user end-point devices.

- Patch Management- Policies and procedures shall be established, and supporting business processes and technical measures implemented, for timely detection of vulnerabilities within organisationally-owned or managed (physical and virtual) applications.

- Mobile Code- Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network.

Cloud Security Controls

Mapping Cloud Controls



- 72 total controls to mitigate the 9 threats (from 12 domains)
- Of which 42 are unique

Cloud Security Controls

Self Assessment Question

1. Is specially designed to deliver important security principles to guide cloud server providers and to assist potential cloud customers in evaluating the overall security risk of a cloud service provider

a) Cloud Control Matrix

b) Service Level Agreement

c) Cloud Security

d) None of these

Answer a

Self Assessment Question

2. Which domain of CCM deals with concerns of compliance for regular internal audits, assessments and reviews of data?

a) The second domain

b) The first domain

c) The third domain

d) All of the above

Answer:**D**

Self Assessment Question

3. In TCI reference architecture, TCI is

a) Third cloud Interface

b) Trusted cloud initiative

c) All of the above

d) None of the above

Answer: b

Self Assessment Question

4. Which of the following is/are not a well-known list of cloud controls?

a) SSAE 16 (formerly SAS 70)

b) CSA CCM

c) ISO 27001:2005

d) FedRAMP

Answer - a

Cloud Security Controls

Self Assessment Question

5. Using a cloud provider for security services is always:

a) Cheaper than doing it on-premise

b) More secure than doing it on-premise

c) The right thing to do

d) A way to impress your boss

Answer - a

Cloud Security Controls

Self Assessment Question

6. Cloud providers ensure that _________via the cloud are secure by implementing testing and acceptance procedures for outsourced or packaged application code.

a) Applications available as a service

b) Infrastructure as a service

c) Platform as a service

d) User as a service

Answer - a

Self Assessment Question

7. Arrange the following in order to be a Cloud Service Provider

a. Identify the threat profile and then decide on a cloud service model
b. Select suitable applications and develop a risk score
c. Build a customized cloud service provider security assessment.
d. Model attack paths to enhance situational awareness
e. Understand the survivability and resiliency of applications

1. c, d, e, b, a
2. b, e, d, c, a
3. a, b, e, d, c
4. a, b, c, d, e

Answer- 3

Self Assessment Question

8. Cloud Security refers to

a) A Broad set of policies

b) Technologies

c) Deployment Controls

d) All of the above

Answer - d

Cloud Security Controls

Self Assessment Question

9. Cloud providers have _________ and __________plans in place to ensure that service can be maintained in case of a disaster or an emergency and that any data lost will be recovered.

a) Business continuity and risk management

b) Business continuity and data recovery

c) Business continuity and project management

Answer - a

Self Assessment Question

10. Cloud providers must enable their customers to comply appropriately with these regulations

a) Payment Card Industry Data Security Standard (PCI)

b) Health Insurance Portability and Accountability Act (HIPAA)

c) Sarbanes-Oxley Act (SOA)

d) All of the above

Answer - d

Cloud Security Controls

Activity

Activity Type: Offline **Duration: 60 Minutes**

Description:

It is said that “TCI increases the value proposition of cloud services within an enterprise model”. Divide the class into two and debate on the topic.

Cloud Security Controls

Subjective Assessment

1) Explain in detail what is cloud computing matrix.
2) Describe in brief what are different domains of cloud computing matrix?
3) Explain what is Trusted Cloud Initiative. How transparency as a service is dependent on it?

Cloud Security Controls

Summary

- In this module, we have studied the cloud control matrix and different domains of cloud security matrix as far as cloud security id concern.
- The Cloud Controls Matrix (CCM) is specially designed to deliver important security principles to guide cloud server providers and to assist potential cloud customers in evaluating the overall security risk of a cloud service provider.
- There are security risks and issues that need to be clearly discussed between both the parties. This clarification should be done before an enterprise considers starting the services of a cloud provider

Cloud Security Controls

External Resources

1. Pethuru Raj - Cloud Enterprise Architecture-– CRC
2. Mark Fenwick, Stefan Wrbka , Flexibility in Modern Business Law: A Comparative Assessment – Springer
3. Federal Cloud Computing: The Definitive Guide for Cloud Service Providers –

Cloud Security Controls

Document Links

Topics	URL	Notes
Domain Security	https://www.techopedia.com/definition/24028/domain-security-policy	This link explains domain security
Security Control	https://www.techopedia.com/definition/29367/cloud-security-control	This link explains security control

Cloud Security Controls

Video Links

Topics	URL	Notes
Preventive and Detective	https://www.youtube.com/watch?v=heOFkInotII	This video explains preventive and defective
Cloud security assessment	https://www.youtube.com/watch?v=giB5D1qacaA	You will learn how to assessment cloud security
Cloud security fundamentals	https://www.youtube.com/watch?v=0lw4KU5wHsk	This video explains Cloud security fundamentals
Deterrent, preventive, detective and corrective security controls for Cloud computing	https://www.youtube.com/watch?v=povA3uaGn-U	This video explains Deterrent, preventive, detective and corrective security controls

Cloud Security Controls

E-Book Links

Topics	URL	Page Number
Securing the Cloud	https://www.fujitsu.com/sg/Images/white-book-of-cloud-security.pdf	All pages