Introduction to Cloud Control Matrix (CCM)

Cloud Security Alliance (CSA) is a registered Foreign Non-Profit Corporation in Washington. It is founded in 2008. It provides fundamental security principles to cloud providers and assist cloud customers to ensure a secure cloud computing environment.

The Cloud Security Alliance Cloud Controls Matrix (CSA CCM) provides a controls framework that gives detailed understanding of security concepts and principles that are applicable to cloud industry. It also highlights its relationship to other industry accepted security standards, regulations and controls frameworks such as ISO27001, ISACA, COBIT, PCIDSS, HIPAA, NIST, etc. The CSA CCM highlights information security control requirements, threats and vulnerabilities in the cloud, and security measures to be implemented in the cloud.

The Cloud Controls Matrix (CCM) comprises of baseline security controls created by the Cloud Security Alliance to help enterprises assess the risk associated with cloud computing. It is a part of the CSA Governance, Risk and Compliance stack and aligned to 16 security domains (in its latest version: Cloud Control Matrix v 3.0.1). Each security domain contains sub-domains and its associated unique control ID, thus, comprising a total of 133 control metrics, as described below:

1. Application & Interface Security (04)

a) Application Security (AIS 01)
APIs shall be designed, developed, deployed, and tested in accordance with leading industry standards e.g. OWASP.
b) Customer Access Requirements (AIS 02)
Identified security, contractual, and regulatory requirements for customer access shall be identified and implemented.
c) Data Integrity (AIS 03)
Data reconciliation and edit checks shall be implemented.
d) Data Security / Integrity (AIS 04)
Policies and procedures shall be established and maintained in support of data security.

2. Audit Assurance & Compliance (03)

a) Audit Planning (AAC 01)
All audit activities shall be agreed upon prior to executing any audits.
b) Independent Audits (AAC 02)
Independent reviews and assessments shall be performed at least annually.
c) Information System Regulatory Mapping (AAC 03)
Relevant standards, regulatory, legal, and statutory requirements shall be identified and mapped to business.

3. Business Continuity Management & Operational Resilience (11)

a) Business Continuity Planning (BCR 01)
A business continuity disaster recovery plan shall be established, documented.

b) Business Continuity Testing (BCR 02)
Business continuity plans shall be tested at planned intervals or upon significant organizational or environmental changes.

c) Datacenter Utilities / Environmental Conditions (BCR 03)
Data center utilities services and environmental conditions shall be secured, monitored, maintained, and tested at planned intervals

d) Documentation (BCR 04)
Information system documents shall be maintained.

e) Environmental Risks (BCR 05)
Physical protection against damage from natural causes and disasters, as well as deliberate attacks shall be designed, and have countermeasures applied.

f) Equipment Location (BCR 06)
All equipments shall be kept away from locations that are subject to environmental risks.

g) Equipment Maintenance (BCR 07)
Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance.

h) Equipment Power Failures (BCR 08)
Backup equipments shall be maintained to withstand damage caused to equipments due to power failures.

i) Impact Analysis (BCR 09)
Business Impact Analysis shall document the impact of any disruption to the organization (cloud provider, cloud consumer).

j) Policy (BCR 10)
Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management.

k) Retention Policy (BCR 04)
Retention period of any critical asset, as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations shall be defined and implemented.

4. Change Control & Configuration Management (05)

a) New Development / Acquisition (CCC 01)
Development and/or acquisition of new data, physical or virtual applications, infrastructure network, and systems components shall be defined and implemented.

b) Outsourced Development (CCC 02)
Change management, release, and testing processes for external business partners within the organization shall be defined and documented.

c) Quality Testing (CCC 03)
Quality change control and testing process with established baselines, testing, and release standards shall be defined and documented.

d) Unauthorized Software Installations (CCC 04)
Installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components shall be restricted.

e) Production Changes (CCC 05)
Technical measures shall be implemented to provide assurance that all production changes directly correspond to a registered change request.

5. Data Security & Information Lifecycle Management (07)

a) Classification (DSI 01)
Data shall be classified by the data owner based on data type, value, sensitivity, and criticality to the organization.
b) Data Inventory / Flows (DSI 02)
Data inventory and data flows shall be maintained for data that is stored(permanently or temporarily) within applications, network and systems components.
c) Ecommerce Transactions (DSI 03)
Electronic ecommerce transactions shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification.
d) Handling / Labeling / Security Policy (DSI 04)
Policies and procedures shall be defined data labeling, handling, and security..
e) Non-Production Data (DSI 05)
Production data shall not be replicated or used in non-production environments.
f) Ownership / Stewardship (DSI 06)
All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.
g) Secure Disposal (DSI 07)
Policies and procedures shall be defined and implemented for the secure disposal and complete removal of data from all storage media.

6. Datacenter Security (09)

a) Asset Management (DCS 01)
Assets must be classified and assigned ownership by defined roles and responsibilities.
b) Controlled Access Points (DCS 02)
Physical security perimeters and checks shall be defined and implemented.
c) Equipment Identification (DCS 03)
Automated equipment identification shall be used as a method of connection authentication.
d) Off-Site Authorization (DCS 04)
Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.
e) Off-Site Equipment (DCS 05)
Policies and procedures shall be defined and implemented for the secure disposal of equipment (by asset type) used outside the organization's premises.
f) Policy (DCS 06)
Policies and procedures shall be defined and implemented.
g) Secure Area Authorization (DCS 07)
Ingress and egress to secure areas shall be restricted and monitored by physical access control mechanisms.
h) Unauthorized Persons Entry (DCS 08)

Ingress and egress point shall be monitored, controlled and, if possible, isolated from data storage and processing facilities

i) User Access (DCS 09)
Physical access to information assets and functions by users and support personnel shall be restricted.

7. Encryption & Key Management (04)

a) Entitlement (EKM 01)
Key handling and management policies shall be defined and implemented.

b) Key Generation (EKM 02)
Policies and procedures shall be defined and implemented for the management of cryptographic keys.

c) Sensitive Data Protection (EKM 03)
Encryption protocols for protection of sensitive data in storage, data in use, and data in transmission shall be defined and implemented.

d) Storage and Access (EKM 04)
Key management and key usage shall be separated duties.

8. Governance and Risk Management (11)

a) Baseline Requirements (GRM 01)
Baseline security requirements shall be defined applications, system and network components

b) Data Focus Risk Assessments (GRM 02)
Risks associated with data governance shall be assessed at planned intervals.

c) Management Oversight (GRM 03)
Managers shall be responsible for complying with security policies, procedures, and standards that are relevant to their area of responsibility.

d) Management Program (GRM 04)
An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented.

e) Management Support/Involvement (GRM 05)
Management shall support information security through clearly-documented direction, ownership and commitment.

f) Policy (GRM 06)
Information security policies and procedures shall be defined and implemented.

g) Policy Enforcement (GRM 07)
A formal disciplinary or sanction policy shall be implemented for employees who have violated security policies and procedures.

h) Policy Impact on Risk Assessments (GRM 08)
Risk assessment results shall include updates to security policies, procedures, standards, and controls.

i) Policy Reviews (GRM 09)
The organization's business leadership shall review the information security policy at planned intervals or as a result of changes to the organization.

j) Risk Assessments (GRM 10)

Risk assessments shall be conducted annually or at planned intervals

k) Risk Management Framework (GRM 11)
Risk Acceptance levels based on risk criteria shall be defined in accordance with reasonable resolution time frames and stakeholder approval.

9. Human Resources (11)

a) Asset Returns (HRS 01)
All organizationally-owned assets shall be returned within an established period.
b) Background Screening (HRS 02)
Employees, contractors, and third parties shall be subject to background verification.
c) Employment Agreements (HRS 03)
Employment agreements shall be defined and duly signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and assets.
d) Employment Termination (HRS 04)
Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.
e) Mobile Device Management (HRS 05)
Risks associated with permitting mobile device access to corporate resources shall be defined and documented as per acceptable-use policies and procedures.
f) Non-Disclosure Agreements (HRS 06)
Non-disclosure or confidentiality agreements shall be identified, documented, and reviewed at planned intervals.
g) Roles / Responsibilities (HRS 07)
Roles and responsibilities of contractors, employees, and third-party users shall be documented and communicated.
h) Technology Acceptable Use (HRS 08)
Usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components shall be defined and documented.
i) Training / Awareness (HRS 09)
All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.
j) User Responsibility (HRS 10)
All personnel shall be made aware of their roles and responsibilities
k) Workspace (HRS 11)
Unattended workspaces shall not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions shall be disabled after an established period of inactivity.

10. Identity & Access Management (13)

a) Audit Tools Access (IAM 01)
Access to, and use of, audit tools shall be appropriately segregated and restricted.
b) Credential Lifecycle / Provision Management (IAM 02)

Identity, entitlement, and access management for all internal corporate and customer (tenant) users shall be defined and documented.

c) Diagnostic / Configuration Ports Access (IAM 03)
User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.

d) Policies and Procedures (IAM 04)
Policies and procedures shall be defined to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access.

e) Segregation of Duties (IAM 05)
User access policies and procedures shall be defined based upon segregation of duties principle.

f) Source Code Access Restriction (IAM 06)
Access to the organization's applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege as per established user access policies and procedures.

g) Third Party Access (IAM 07)
Risks posed by business processes requiring third-party access to the organization's information systems and data shall be identified and documented.

h) Trusted Sources (IAM 08)
Trusted users shall be explicitly defined and documented.

i) User Access Authorization (IAM 09)
User access to data and organizationally-owned or managed applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted

j) User Access Reviews (IAM 10)
User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals.

k) User Access Revocation (IAM 11)
De-provisioning of user access to data and organizationally-owned or managed applications, infrastructure systems, and network components, shall be implemented based on user's change in status.

l) User ID Credentials (IAM 12)
Internal corporate or customer (tenant) user account credentials shall be restricted.

m) Utility Programs Access (IAM 13)
Utility programs access shall be restricted.

11. Infrastructure & Virtualization Security (13)

a) Audit Logging / Intrusion Detection (IVS 01)
Audit logs shall be maintained and protected adhering to applicable legal, statutory or regulatory compliance requirements.

b) Change Detection (IVS 02)
Any changes to virtual machine images shall be logged and an alert shall be raised regardless of their running state.

c) Clock Synchronization (IVS 03)
System clocks shall be synchronized to facilitate tracing and reconstitution of activity timelines.

d) Information System Documentation (IVS 04)
Information System details comprising its availability, quality, capacity, performance and resources shall be defined and measured as per agreed SLAs.

e) Vulnerability Management (IVS 05)
Vulnerability assessment tools or services shall be configured and implemented.

f) Network Security (IVS 06)
Network Security shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections.

g) OS Hardening and Base Controls (IVS 07)
Operating systems shall be hardened to provide only necessary ports, protocols, and services to meet business needs.

h) Production / Non-Production Environments (IVS 08)
Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets.

i) Segmentation (IVS 09)
System and network components, shall be designed, developed, deployed, and configured such that provider and customer access is appropriately segmented from other users.

j) VM Security - Data Protection (IVS 10)
Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers.

k) Hypervisor Hardening (IVS 11)
Hypervisor hardening shall be implemented as per agreed security controls.

l) Wireless Security (IVS 12)
Wireless network environments access shall be restricted.

m) Network Architecture (IVS 13)
Network architecture diagrams shall be documented and any further changes shall undergo a formal change management process.

12. Interoperability & Portability (05)

a) APIs (IPY 01)
The provider shall use published APIs.

b) Data Request (IPY 02)
All structured and unstructured data shall be provided to customer upon request, in an industry-standard format.

c) Policy & Legal (IPY 03)
Policies, procedures, and mutually-agreed upon provisions and/or terms shall be defined and documented.

d) Standardized Network Protocols (IPY 04)
The provider shall use secure standardized network protocols for the import and export of data.

e) Virtualization (IPY 05)
Industry-recognized virtualization platform and standard virtualization formats shall be used by the cloud provider.

13. Mobile Security (20)

a) Anti-Malware (MOS 01)
Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.

b) Application Stores (MOS 02)
Approved application stores shall be defined and documented for mobile devices accessing or storing provider managed data.

c) Approved Applications (MOS 03)
Approved list of applications for mobile devices shall be defined and documented.

d) Approved Software for BYOD (MOS 04)
Approved Software for BYOD shall be defined and documented in BYOD policy and supporting awareness training.

e) Awareness and Training (MOS 05)
Mobile device policy and requirements shall be through the company's security awareness and training program.

f) Cloud Based Services (MOS 06)
All cloud-based services used by the company's mobile devices or BYOD shall be documented and communicated to mobile users.

g) Compatibility (MOS 07)
The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.

h) Device Eligibility (MOS 08)
The BYOD policy shall define the device eligibility requirements for BYOD usage.

i) Device Inventory (MOS 09)
An inventory of all mobile devices shall be maintained.

j) Device Management (MOS 10)
A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.

k) Encryption (MOS 11)
The mobile device policy shall enforce encryption, either for the entire device or for data identified as sensitive

l) Jailbreaking and Rooting (MOS 12)
The mobile device policy shall restrict the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting).

m) Legal (MOS 13)
BYOD policy shall clearly state the loss of non-company data in case that a wipe of the device is required.

n) Lockout Screen (MOS 14)
BYOD and/or company-owned devices shall be configured with an automatic lockout screen.

o) Operating Systems (MOS 15)
Changes to mobile device operating systems, patch levels, and/or applications shall be managed through change management processes.

p) Passwords (MOS 16)
Password policy shall be documented and communicated on all company devices or devices approved for BYOD usage.

q) Policy (MOS 17)
The mobile device policy shall enforce backup of data, restrict usage of unapproved application stores, and require the use of anti-malware software.

r) Remote Wipe (MOS 18)
BYOD or a company-assigned mobile device shall permit remote wipe of device by company's corporate IT.

s) Security Patches (MOS 19)
All mobile devices shall be configured with latest security patches installed upon general release by the device manufacturer or carrier.

t) Users (MOS 20)
Approved list of systems and servers shall be documented that are allowed for use or access on a BYOD device.

14. Security Incident Management, E-Discovery, & Cloud Forensics (05)

a) Contact / Authority Maintenance (SEF 01)
Points of contact of applicable regulatory authorities and other legal jurisdictional authorities shall be maintained.

b) Incident Management (SEF 02)
Formal Incident Management process shall be implemented to triage security-related events and ensure timely and thorough incident resolution.

c) Incident Reporting (SEF 03)
Information security events shall be reported through predefined communication channels in a timely manner.

d) Incident Response Legal Preparation (SEF 04)
Forensic procedures, including chain of custody, shall be followed for the presentation of evidence to support legal action subject to the relevant jurisdiction after an information security incident.

e) Incident Response Metrics (SEF 05)
Process shall be implemented to monitor and quantify the types, volumes, and costs of information security incidents.

15. Supply Chain Management, Transparency, and Accountability (09)

a) Data Quality and Integrity (STA 01)
Separation of duties, role-based access, and least-privilege access for all personnel within their supply chain shall be implemented.

b) Incident Reporting (STA 02)
Security incident information shall be available to all affected customers and providers.

c) Network / Infrastructure Services (STA 03)
Infrastructure network and system components shall be designed, developed, and deployed in accordance with agreed SLAs.

d) Provider Internal Assessments (STA 04)
The provider shall perform scheduled annual internal assessments of its policies, procedures, and supporting measures and metrics.

e) Supply Chain Agreements (STA 05)

Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall be documented and enforced.

f) Supply Chain Governance Reviews (STA 06)
Providers shall review the risk management and governance processes of their partners.

g) Supply Chain Metrics (STA 07)
Consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream) shall be performed.

h) Third Party Assessment (STA 08)
Third part assessment shall be periodically conducted as per agreed intervals.

i) Third Party Audits (STA 09)
Third-party service providers shall undergo periodic checks at agreed intervals.

16. Threat and Vulnerability Management (03)

a) Anti-Virus / Malicious Software (TVM 01)
Execution of malware on organizationally-owned or managed user end-point devices and IT infrastructure network and systems components shall be restricted.

b) Vulnerability / Patch Management (TVM 02)
Formal Vulnerability and Patch Management process shall be implemented for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components.

c) Mobile Code (TVM 03)
Execution of unauthorized mobile code shall be prevented on organizationally-owned or managed user end-point devices, infrastructure network and systems components.