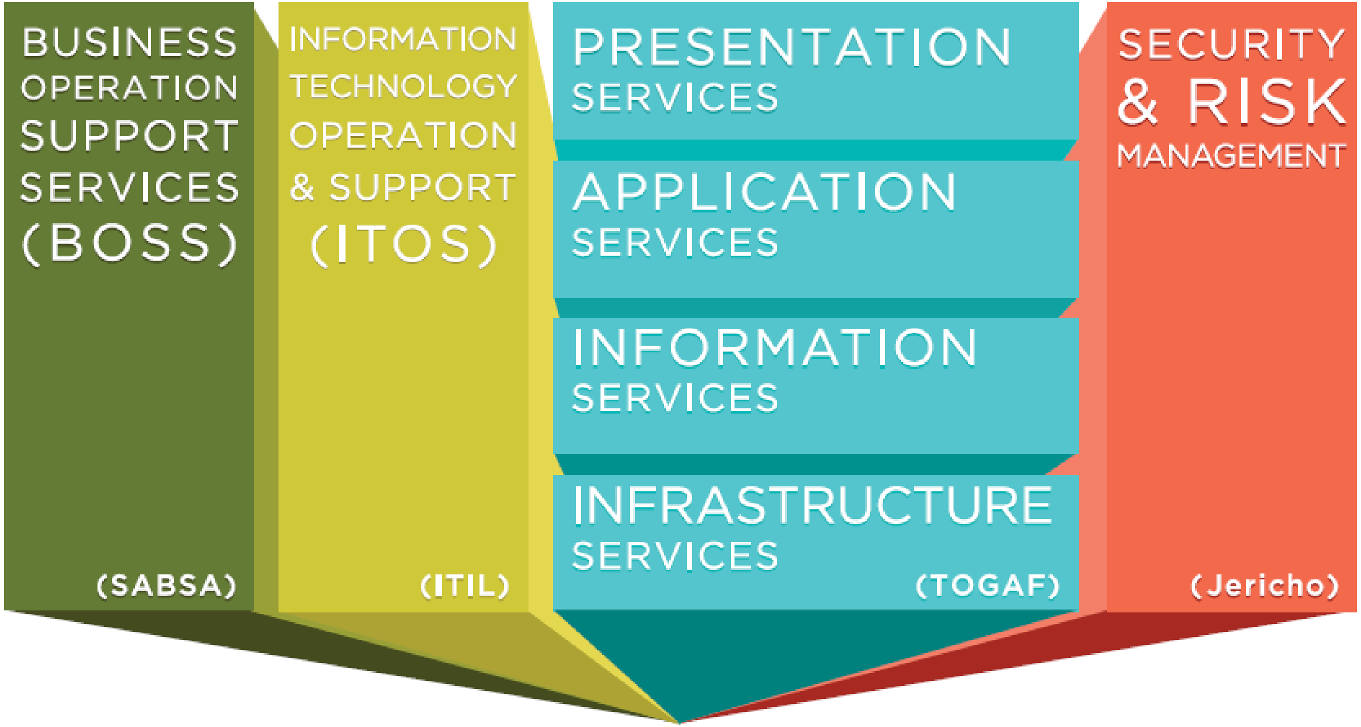
Cloud Security Alliance TCI Reference Architecture



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)

Legend:

CSA: Cloud Security Alliance

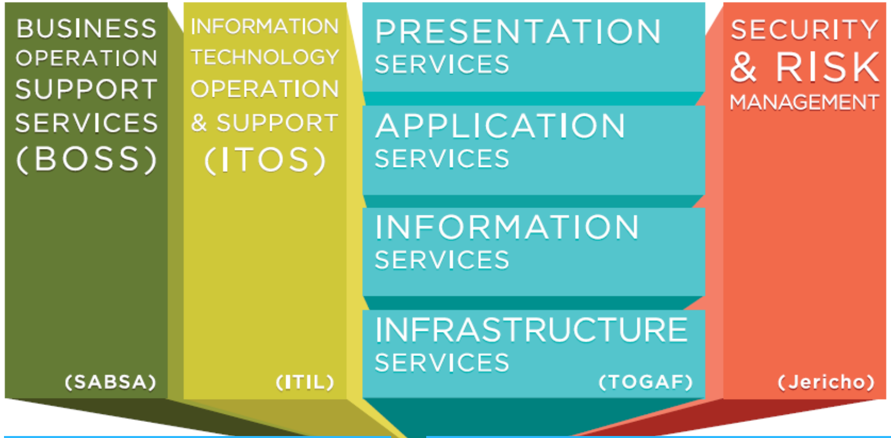
TCI: Trusted Cloud Initiative

Source: https://cloudsecurityalliance.org/wp-content/uploads/2011/10/TCI_Whitepaper.pdf

Cloud Security Alliance TCI Reference Architecture

BOSS Services:

- Compliance
- Data Governance
- Operational Risk Management
- Human Resources Security
- Security Monitoring Services
- Legal Services
- Internal Investigation


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)

SRM Services:

- Governance Risk and Compliance
- Information Security Management
- Privilege Management Infrastructure
- Threat and Vulnerability Management
- Infrastructure Protection Services
- Data Protection
- Policies and Standards

ITOS Services:

- IT Operations
- Service Delivery
- Service Support
- Incident Management
- Problem Management
- Knowledge Management
- Change Management
- Release Management

Presentation Services:

- Presentation Modality
- Presentation Platform

Application Services:

- Development Process
- Security Knowledge Lifecycle
- Programming Interfaces
- Integration Middleware
- Connectivity & Delivery
- Abstraction

Information Services:

- User Directory Services
- Security Monitoring Data Management
- Service Delivery Data Management
- Service Support Data Management
- Data Governance Data Management
- Risk Management Data Management
- ITOS Data Management
- BOSS Data Management
- Reporting Services

Infrastructure Services:

- Facility Services
- Servers
- Storage Services
- Network Services
- Availability Services
- Patch Management
- Equipment Maintenance
- Virtualization (Desktop, Storage, Server, Network)

Source: https://cloudsecurityalliance.org/wp-content/uploads/2011/10/TCI_Whitepaper.pdf

CSA Cloud Control Matrix CCM v3.0.1; 16 Domains

1. **AIS**: Application & Interface Security (4)
2. **AAC**: Audit Assurance & Compliance (3)
3. **BCR**: Business Continuity Management & Operational Resilience (11)
4. **CCC**: Change Control & Configuration Management (5)
5. **DSI**: Data Security & Information Lifecycle Management (7)
6. **DCS**: Datacenter Security (9)
7. **EKM**: Encryption & Key Management (4)
8. **GRM**: Governance and Risk Management (11)
9. **HRS**: Human Resources (11)
10. **IAM**: Identity & Access Management (13)
11. **IVS**: Infrastructure & Virtualization Security (13)
12. **IPY**: Interoperability & Portability (5)
13. **MOS**: Mobile Security (20)
14. **SEF**: Security Incident Management, E-Discovery & Cloud Forensics (5)
15. **STA**: Supply Chain Management, Transparency and Accountability (9)
16. **TVM**: Threat and Vulnerability Management (3)

Source: https://cloudsecurityalliance.org/research/ccm/

Legend:
CSA: Cloud Security Alliance
CCM: Cloud Control Matrix
(Number of controls) for each Domain

CSA Cloud Control Matrix CCM v3.0.1; 133 Controls

Application & Interface Security (AIS)

- AIS-01: Application Security
- AIS-02: Customer Access Requirements
- AIS-03: Data Integrity
- AIS-04: Data Security / Integrity

Audit Assurance & Compliance (AAC)

- AAC-01: Audit Planning
- AAC-02: Independent Audits
- AAC-03: Information System Regulatory Mapping

Business Continuity Management & Operational Resilience (BCR)

- BCR-01: Business Continuity Planning
- BCR-02: Business Continuity Testing
- BCR-03: Datacenter Utilities / Environmental Conditions
- BCR-04: Documentation
- BCR-05: Environmental Risks
- BCR-06: Equipment Location
- BCR-07: Equipment Maintenance
- BCR-08: Equipment Power Failures
- BCR-09: Impact Analysis
- BCR-10: Policy
- BCR-11: Retention Policy

Change Control & Configuration Management (CCC)

- CCC-01: New Development / Acquisition
- CCC-02: Outsourced Development
- CCC-03: Quality Testing
- CCC-04: Unauthorized Software Installations
- CCC-05: Production Changes

Data Security & Information Lifecycle Management (DSI)

- DSI-01: Classification
- DSI-02: Data Inventory / Flows
- DSI-03: eCommerce Transactions
- DSI-04: Handling / Labeling / Security Policy
- DSI-05: Non-Production Data
- DSI-06: Ownership / Stewardship
- DSI-07: Secure Disposal

Source: https://cloudsecurityalliance.org/research/ccm/

CSA Cloud Control Matrix CCM v3.0.1; 133 Controls

Datacenter Security (DCS)

- DCS-01: Asset Management
- DCS-02: Controlled Access Points
- DCS-03: Equipment Identification
- DCS-04: Off-Site Authorization
- DCS-05: Off-Site Equipment
- DCS-06: Policy
- DCS-07: Secure Area Authorization
- DCS-08: Unauthorized Persons Entry
- DCS-09: User Access

Encryption & Key Management (EKM)

- EKM-01: Entitlement
- EKM-02: Key Generation
- EKM-03: Sensitive Data Protection
- EKM-04: Storage and Access

Governance and Risk Management (GRM)

- GRM-01: Baseline Requirements
- GRM-02: Data Focus Risk Assessments
- GRM-03: Management Oversight
- GRM-04: Management Program
- GRM-05: Management Support/Involvement
- GRM-06: Policy
- GRM-07: Policy Enforcement
- GRM-08: Policy Impact on Risk Assessments
- GRM-09: Policy Reviews
- GRM-10: Risk Assessments
- GRM-11: Risk Management Framework

Source: https://cloudsecurityalliance.org/research/ccm/

CSA Cloud Control Matrix CCM v3.0.1; 133 Controls

Human Resources (HRS)

- HRS-01: Asset Returns
- HRS-02: Background Screening
- HRS-03: Employment Agreements
- HRS-04: Employment Termination
- HRS-05: Mobile Device Management
- HRS-06: Non-Disclosure Agreements
- HRS-07: Roles / Responsibilities
- HRS-08: Technology Acceptable Use
- HRS-09: Training / Awareness
- HRS-10: User Responsibility
- HRS-11: Workspace

Identity & Access Management (IAM)

- IAM-01: Audit Tools Access
- IAM-02: Credential Lifecycle / Provision Management
- IAM-03: Diagnostic / Configuration Ports Access
- IAM-04: Policies and Procedures
- IAM-05: Segregation of Duties
- IAM-06: Source Code Access Restriction
- IAM-07: Third Party Access
- IAM-08: Trusted Sources
- IAM-09: User Access Authorization
- IAM-10: User Access Reviews
- IAM-11: User Access Revocation
- IAM-12: User ID Credentials
- IAM-13: Utility Programs Access

Source: https://cloudsecurityalliance.org/research/ccm/

CSA Cloud Control Matrix CCM v3.0.1; 133 Controls

Infrastructure & Virtualization Security (IVS)

- IVS-01: Audit Logging / Intrusion Detection
- IVS-02: Change Detection
- IVS-03: Clock Synchronization
- IVS-04: Information System Documentation
- IVS-05: Management - Vulnerability Management
- IVS-06: Network Security
- IVS-07: OS Hardening and Base Controls
- IVS-08: Production / Non-Production Environments
- IVS-09: Segmentation
- IVS-10: VM Security - vMotion Data Protection
- IVS-11: VMM Security - Hypervisor Hardening
- IVS-12: Wireless Security
- IVS-13: Network Architecture

Interoperability & Portability (IPY)

- IPY-01: APIs
- IPY-02: Data Request
- IPY-03: Policy & Legal
- IPY-04: Standardized Network Protocols
- IPY-05: Virtualization

Mobility Security (MOS)

- MOS-01: Anti-Malware
- MOS-02: Application Stores
- MOS-03: Approved Applications
- MOS-04: Approved Software for BYOD
- MOS-05: Awareness and Training
- MOS-06: Cloud Based Services
- MOS-07: Compatibility
- MOS-08: Device Eligibility
- MOS-09: Device Inventory
- MOS-10: Device Management
- MOS-11: Encryption
- MOS-12: Jailbreaking and Rooting
- MOS-13: Legal
- MOS-14: Lockout Screen
- MOS-15: Operating Systems
- MOS-16: Passwords
- MOS-17: Policy
- MOS-18: Remote Wipe
- MOS-19: Security Patches
- MOS-20: Users

Source: https://cloudsecurityalliance.org/research/ccm/

CSA Cloud Control Matrix CCM v3.0.1; 133 Controls

Security Incident Management, E-Discovery & Cloud Forensics (SEF)

- SEF-01: Contact / Authority Maintenance
- SEF-02: Incident Management
- SEF-03: Incident Reporting
- SEF-04: Incident Response Legal Preparation
- SEF-05: Incident Response Metrics

Supply Chain Management, Transparency and Accountability (STA)

- STA-01: Data Quality and Integrity
- STA-02: Incident Reporting
- STA-03: Network / Infrastructure Services
- STA-04: Provider Internal Assessments
- STA-05: Supply Chain Agreements
- STA-06: Supply Chain Governance Reviews
- STA-07: Supply Chain Metrics
- STA-08: Third Party Assessment
- STA-09: Third Party Audits

Threat and Vulnerability Management (TVM)

- TVM-01: Anti-Virus / Malicious Software
- TVM-02: Vulnerability / Patch Management
- TVM-03: Mobile Code

Source: https://cloudsecurityalliance.org/research/ccm/