

Welcome to Latest Version of the Cloud Controls Matrix, CCM v3.0.1!

ABOUT THE CSA CLOUD CONTROLS MATRIX



- Provides fundamental security principles to guide cloud vendors and to assist cloud customers in assessing the overall security risk of a cloud provider
- Strengthens information security control environments by delineating control guidance by service provider and consumer, and by differentiating according to cloud model type and environment
- Provides a controls framework in 16 domains that are cross-walked to other industry-accepted security standards, regulations, and controls frameworks to reduce audit complexity
- Seeks to normalize security expectations, cloud taxonomy and terminology, and security measures implemented in the cloud

ABOUT THE CCM VERSION CONTROL



Version updates named as a 0.0.X release will include:

- New and updated mappings, and/or
- minor changes in control specification language.

WHAT'S NEW IN THIS VERSION!

- New or updated mappings to the following
 - + AICPA 2014 Trust Services Criteria
 - + Canada PIPEDA (Personal Information Protection Electronic Documents Act)
 - + COBIT 5.0
 - + COPPA (Children's Online Privacy Protection Act)
 - + CSA Enterprise Architecture
 - + ENISA (European Network Information and Security Agency) Information Assurance Framework
 - + European Union Data Protection Directive 95/36/EC
 - + FERPA (Family Education and Rights Privacy Act)
 - + HIPAA/HITECH act and the Omnibus Rule
 - + ISO/IEC 27001:2013
 - + ITAR (International Traffic in Arms Regulation)
 - + Mexico - Federal Law on Protection of Personal Data Held by Private Parties
 - + NIST SP800-53 Rev 3 Appendix J
 - + NZISM (New Zealand Information Security Manual)
 - + ODCA (Open Data Center Alliance) Usage Model PAAS Interoperability Rev. 2.0
 - + PCI DSS v3
- Consolidation of redundant controls
- Rewritten controls for clarity of intent, STAR enablement, and SDO alignment



Cloud Controls Matrix v3.0.1

Quick Stats

FOR MORE INFORMATION:
<https://cloudsecurityalliance.org/research/ccm>
<https://blog.cloudsecurityalliance.org/ccm/>
ccm-leadership@cloudsecurityalliance.org

CCM v3.0.1 DOMAINS

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

136 CONTROLS
Cloud Controls Matrix v3.0



133 CONTROLS
Cloud Controls Matrix v3.0.1

CONTROL SPECIFICATION NUMBERING UPDATES

- **BCR-10** (Business Continuity Management & Operational Resilience *Management Program*) has been removed and consolidated in **BCR-01**.
- **BCR-11** (Business Continuity Management & Operational Resilience *Policy*) has been moved to the **BCR-10** Control Domain.
- **BCR-12** (Business Continuity Management & Operational Resilience *Retention Policy*) has been moved to the **BCR-11** Control Domain.
- **DSI-05** (Data Security & Information Lifecycle Management *Information Leakage*) has been removed since data loss/leakage is covered in other controls such as **GRM-02**, **GRM-04**, and **DCS-08**.
- **DSI-06** (Data Security & Information Lifecycle Management *Non-Production Data*) has been moved to the **DSI-05** Control Domain.
- **DSI-07** (Data Security & Information Lifecycle Management *Ownership / Stewardship*) has been moved to the **DSI-06** Control Domain.
- **DSI-08** (Data Security & Information Lifecycle Management *Secure Disposal*) has been moved to the **DSI-07** Control Domain.
- **GRM-12** (Governance and Risk Management *Risk Management Framework*) has been removed as it was addressed in **GRM-11**.
- **HRS-05** (Human Resources *Industry Knowledge / Benchmarking*) has been removed and assumed as regular practices.
- **HRS-06** (Human Resources *Mobile Device Management*) has been moved to the **HRS-05** Control Domain.
- **HRS-07** (Human Resources *Non-Disclosure Agreements*) has been moved to the **HRS-06** Control Domain.
- **HRS-08** (Human Resources *Roles / Responsibilities*) has been moved to the **HRS-07** Control Domain.
- **HRS-09** (Human Resources *Technology Acceptable Use*) has been moved to the **HRS-08** Control Domain.
- **HRS-10** (Human Resources *Training / Awareness*) has been moved to the **HRS-09** Control Domain.
- **HRS-11** (Human Resources *User Responsibility*) has been moved to the **HRS-10** Control Domain.
- **HRS-12** (Human Resources *Workspace*) has been moved to the **HRS-11** Control Domain.
- **IVS-13** (Infrastructure & Virtualization Security *Network Architecture*) has been added. This domain has been split off from the **IVS-06** Control Domain.