EDM Council
Cloud CDMC Working Group
Q3 2021 Update

Confidential EDM Council Proprietary Document.
For distribution solely within CDMC participating companies.
EDM Council Overview

Mission: *Elevate the practice of data and analytics management and support the role of the data professional*

Principles:

We believe in a **responsible data-driven** organization and establishing **data literacy for all**.

We advocate **industry collaboration** to provide data management and analytics research, best practices, standards, training and education.

We are the **neutral, non-profit** industry forum for companies and their data & analytics professionals.

---

Established 2005

Worldwide
Americas, Europe, Africa, Asia, Australia

250+ Member Firms
Cross-industry, including Regulators

10,000+ Professionals
EDM Council's Areas of Advocacy

**Best Practices**
- DCAM & Cloud CDMC
- ESG Data
- Data ROI

**Driving Standards**
- Knowledge Graph
- Industry Ontologies
- Shared Lab

**Training & Certification**
- Virtual & eLearning Courses
- EDMWebinars & Events

**Research & Benchmarking**
- Global Industry Study
- Life Sciences
- Data Sharing

**Regulatory Engagement**
- Regulators participate in the agenda
- Many regulators are members

**Networking**
- EDMConnect Community
- DataVision, CDO Summit
- Workgroups & Forums
Data Management Capability Assessment Model

WHO?
• Developed via member collaboration
• 62% of Council members using frameworks use DCAM

WHAT’S IN DCAM?
• 8 components, 38 Capabilities, 136 Sub-capabilities
• Members flexibly apply to their organization
• Includes: Data Supply Chain, Advanced Analytics, Data Ethics and Responsible AI/ML

USED FOR:
• Program Initiation & Funding
• Team Training & Common Language
• Assessments & Benchmarking
Cloud Data Management Capability (CDMC)

CDMC Working Group

Cloud Challenges

• **Inefficiency**: data, technology, regulatory and planning challenges on nearly every cloud implementation

• **93% of firms** use 2 or more cloud providers*

CDMC Group Objectives

1. Align key cloud data controls to meet regulatory obligations for Sensitive Data
2. Define consistent best practices for a hybrid-cloud world
3. Accelerate Cloud Adoption with comprehensive framework modeled after the DCAM Framework

* Source: Flexera, 2020 State of the Cloud
CDMC: Industry Engagement

70+ Leading firms and 226 participants actively participating since May 2020

CDMC Working Group

- Morgan Stanley
- J.P. Morgan
- Standard Chartered
- KPMG
- UBS
- HSBC
- Citi
- Goldman Sachs
- PayPal
- Freddie Mac
- Wells Fargo
- TS ICAP
- Northern Trust
- Barclays
- Deutsche Bank
- Lloyds Bank
- BNP Paribas
- Credit Suisse
- Nasdaq
- Societe Generale

Cloud & Technology Provider Certification

- AWS
- Microsoft Azure
- Google Cloud
- IBM Cloud
- Snowflake
- Collibra
- Informatica
- BigID
- Data.world
- Privitar

Regulatory Engagement

- US: Federal Reserve, OCC, FDIC, NCUA, NAIC
- Canada: OSFI, BoC, CDIC
- UK: BoE, FCA, IOC
- EU: EBA, ECB, DORA Act
- Germany: BaFin
- Swiss: FinMA
- Japan: FSA
- Australia: APRA
- Singapore: MAS
- India: RBI, SEBI
- Africa/Middle East regulators
- Others

Go-to-market Support

- Training Courses
- Cloud Service Certification
- Open Source Tools
- CDMC Authorized Partner Program

CDMC Working Group Publication on track for Q3 2021
### CDMC Capabilities: Requirements & Automated Controls

<table>
<thead>
<tr>
<th>Component</th>
<th>Capability</th>
<th>Sub-Capability</th>
<th>CDMC Automation Checklist (DRAFT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Governance &amp; Accountability</td>
<td>1.1 The Cloud Data Management business case is defined and measurable</td>
<td>1.1.1 Cloud data management business cases are governed and syndicated</td>
<td>Ownership field required for specified classifications (eg PII, MNPI, ISC=HR(C))</td>
</tr>
<tr>
<td></td>
<td>1.2 Data ownership established for both migrated &amp; cloud-generated data</td>
<td>1.2.1 Data Owner roles and responsibilities are defined and agreed</td>
<td>Authorisation field required on cataloged data assets for specified classifications (eg PII, MNPI, ISC=HR(C))</td>
</tr>
<tr>
<td></td>
<td>1.3 Data sourcing and consumption are governed and supported by automation</td>
<td>1.3.1 Data sourcing is managed and authorized</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.4 Data Sovereignty and Cross-Border Data Movement are actively managed</td>
<td>1.3.2 Data consumption is governed and supported by automation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.1 Data catalogues are implemented, used and interoperable</td>
<td>1.4.1 Jurisdictional location of data is tracked and reported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.2 Data classifications are defined and used</td>
<td>1.4.2 Data Sovereignty and Cross-Border Data movement risks are mitigated</td>
<td></td>
</tr>
<tr>
<td>2. Data Cataloguing &amp; Classification</td>
<td>2.1 Data catalogues are implemented, used and interoperable</td>
<td>2.1.1 Data cataloguing is defined, scoped and actively used</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.2 Data classifications are defined and used</td>
<td>2.1.2 Metadata is discoverable, enriched, managed and exposed in Data Catalogues</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.1 Data entitlements are managed, enforced and tracked</td>
<td>2.1.3 Data catalogues are interoperable across multi and hybrid cloud environments</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.2 Ethical access, use, and outcomes of data are managed</td>
<td>2.2.1 Data classifications are defined and approved</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Data is secured, and controls are evidenced</td>
<td>2.2.2 Data classifications are applied and actively used</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4.1 A data privacy framework is defined and operational</td>
<td>4.1.1 Encryption policies are defined and enforced for data at rest, in motion, and in use</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Data quality is managed</td>
<td>4.1.2 Implementation of data security controls is evidenced</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5.2 The data lifecycle is planned and managed</td>
<td>4.1.3 Data obfuscation techniques are defined, scoped and applied</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Data provenance and lineage are understood</td>
<td>4.1.4 A Data Loss Prevention regime is in place</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6.2 Technical design principles are established and applied</td>
<td>4.2.1 A data privacy framework is defined and agreed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6.2.1 Data provenance traceability is automatically recorded and tracked</td>
<td>4.2.2 The data privacy framework is operational</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6.2.2 Data lineage reporting and visualization</td>
<td>6.1.1 Multi-environment lineage discovery is automated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6.2.3 Data protection and management are supported</td>
<td>6.1.2 Data provenance tracking and change management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6.2.4 Principles for data availability and resilience are defined and applied</td>
<td>6.1.3 Data lineage reporting and visualization</td>
<td></td>
</tr>
</tbody>
</table>
Cloud Data Management Capabilities (CDMC) 14 Key Controls

1. **Data Control Compliance Metric** must be produced for all data assets containing sensitive data.

2. The **Ownership field** in a data catalog must be populated for all sensitive data.

3. A register of **Authoritative Sources and Authorized Distributors** must be populated for all data assets containing sensitive data.

4. The **Data Sovereignty and Cross-Border Movement** of sensitive data must be recorded, auditable and controlled according to defined policy.

5. **Cataloguing** must be automated for all data at point of creation or ingestion.

6. **Classification** must be automated for all data at point of creation or ingestion and must be always on.

7. **Entitlements and Access for Sensitive Data** must be defaulted to creator and owner and all access must be tracked.

8. **Data Consumption Purpose** is required for all Data Sharing Agreements involving sensitive data.

9. **Appropriate Security Controls** must be enabled for sensitive data and evidence must be recorded.

10. **Data Privacy Impact Assessments** must be automatically triggered for all personal data according to its jurisdiction.

11. **Data Quality Measurement** must be enabled for sensitive data with metrics distributed when available.

12. **Data Retention, Archiving and Purging** must be managed according to a defined retention schedule.

13. **Data Lineage** information must be available for all sensitive data.

14. **Cost Metrics** directly associated with the use, storage and movement of data must be available in the catalog.

**Sensitive Data** includes classifications such as:
- Personal Information (PI) / Sensitive Personal Data
- Personally Identifiable Information (PII)
- Client Identifiable Information
- Material Non-Public Information (MNPI)
- Specific Information Sensitivity Classifications (such as ‘Highly Restricted’ and ‘Confidential’)
- Critical Data Elements used for important business processes
- Licensed data

**CDMC 14 Controls Free Download License**

CONFIDENTIAL | © 2021 EDM Council Inc.
### CDMC Framework – Structure

#### Sub-Capability Description

<table>
<thead>
<tr>
<th>Sub-Capability</th>
<th>Description</th>
<th>Objectives</th>
<th>Advice for Data Practitioners</th>
<th>Advice for CSPs and Technology Providers</th>
<th>Questions that need to be answered</th>
<th>Auditable “Artifacts of Evidence”</th>
<th>Scoring Guidance to measure compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAPABILITY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUB-CAPABILITY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OBJECTIVES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ADVICE FOR DATA PRACTITIONERS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ADVICE FOR CLOUD SERVICE AND TECHNOLOGY PROVIDERS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QUESTIONS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ARTIFACTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCORING</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CDMC Deliverables Availability

**July 2021: 14 CDMC Key Controls & Automations**
- First CDMC Industry Deliverable published 7 July 2021
- Auditable, evidence-based Key CDMC Controls & Automations for managing and protecting sensitive data
- 20-page document
- Summarizes and elaborates on key controls in Framework

  **DOWNLOAD 14 CDMC KEY CONTROLS:**
  - [https://edmcouncil.org/page/cdmc-14-key-controls-and-automation](https://edmcouncil.org/page/cdmc-14-key-controls-and-automation)

**September 2021: Complete CDMC Framework**
- Comprehensive 150+ page document
- 6 Components, 14 capabilities, 37 sub-capabilities
  - Incorporates the 14 Key Controls & Automations
- Availability of 2-day training course
- Other Online Digital Support tools
CDMC Authorized Partner (CAP) Program Modeled after DCAM Authorized Partner Program (DAP)

- **Objective**: Provide comprehensive CDMC Training, Assessment and Certification Services
- **Approach**: CDMC Program Modeled after the DCAM Authorized Partner (DAP) Program
  - DAP Program started 2015 and today comprises 30 DAP Partner companies globally
  - DAP Program globally includes 600+ trained & accredited consultants and 20+ certified master trainers

CDMC Authorized (CAP) Partner Program – Industry Support Services

1. **CDMC Training** – to provide training classes to companies or internal associates
2. **CDMC “Readiness Assessments”** – conducted by CAP Partner with CDMC trained resources for assessing either the 14 CDMC Key Controls and/or for the Full CDMC Framework
3. **CDMC “Certification Assessments”** – CAP Partner to certify achievement of CDMC Capabilities
   - CDMC Certification for CSP/Tech Platform offerings being compliant to CDMC 14 Key Controls & Automations
   - CDMC Certification for end Companies across full CDMC Framework
4. **CDMC Trusted Brand** – use of CDMC logo for industry awareness and trust in cloud adoption
CDMC Go-To-Market Support - Roadmap & Timeline

Q1 2021 – Organize, Plan & Establish CDMC Support Program
• Organize and develop plan
• Establish CAP Program Agreement (for Assessments & Training) with Early Development Partner Program Commercial Benefits
• Form Training Development Committee with and commence development with early CAP Partners cross segment
• Plan for Certification Programs for both Institution and Application/Data/Platform Providers

Q2 2021 – Finalize Development of CDMC Framework, Training Materials & Authorized Partner Program
• Validate Training Template leveraging completed Data Classification & Cataloging component (post editorial review)
• Utilize Training Template and sequence development of other CDMC components as they come available
• Continue to develop Certification Programs for both Institution and Application/Data/Platform Providers
• Launch CDMC Authorized Partner Program (CAP) – first to market CDMC Partners

• Publishing CDMC Assessor’s Guide (the Framework) free download available to include scoring guide & glossary of terms
• Virtual CDMC Training class Available – develop training materials for eLearning production and certification exam development
• Core Training, assessment approach operational to meet industry support objective

Q4 2021 – CDMC Broader Industry Roll-out
• Continue CDMC rollout to other industry verticals
• Certification Exam Operational on eLearning platform – Q4 21 development and Q1 22 availability
• Additional CAP Partners trained & certified and offering training, assessment and certification services
# CDMC: Accelerating Trusted Cloud Adoption

**CDMC Industry Objective:**

*Build Trust, Confidence, and Dependability for Cloud Adoption*

<table>
<thead>
<tr>
<th><strong>Application, Technology &amp; Data Providers</strong></th>
<th><strong>Consultants &amp; Systems Integrators (SI)</strong></th>
<th><strong>Cloud Service Providers (CSP)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorporates certified CDMC capabilities and controls into services and solutions to ensure high degree of reliability and operational effectiveness</td>
<td>CDMC enables training &amp; assessments, gap analysis, strategy development, and execution services for end clients adopting cloud</td>
<td>CDMC requirements and controls can be automated into CSP platforms which accelerates adoption and provides market confidence</td>
</tr>
</tbody>
</table>

**Regulators**

CDMC provides industry guidance for auditing and validating key cloud controls, especially for sensitive data