

# EDM Webinar

## Reimagining Data Governance in the Cloud

A conversation with



**Oli Bage**  
Head of Architecture,  
Data & Analytics  
LSEG



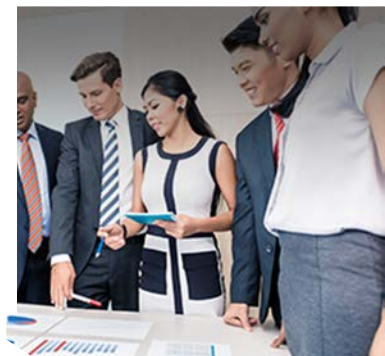
**Mojgan Ahmadi**  
Principal Solutions Architect  
AWS



**Jen Code**  
Principal Cloud Governance  
AWS



**Christopher Glover**  
Field CTO  
BigID



# Moderated by **Mike Meriton**

## Co-Founder & COO, EDM Council

- Joined EDM Council full-time 2015 to lead Industry Engagement
- EDM Council Co-Founder & First Chairman (2005-2007)
- EDM Council Finance Board Chair (2007-2015)
- Former CEO GoldenSource (2002-2015)
- Former Executive for D&B Software and Oracle
- FinTech Innovation Lab – Executive Mentor (2011 – Present)



# Today's panel

Moderator



**Mike Meriton**

Co-Founder & COO  
EDM Council



**Oli Bage**

Head of Architecture,  
Data & Analytics  
LSEG



**Jen Code**

Principal Cloud  
Governance  
AWS



**Mojgan Ahmadi**

Principal Solutions  
Architect  
AWS



**Christopher Glover**

Field CTO  
BigID



Customer Need



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

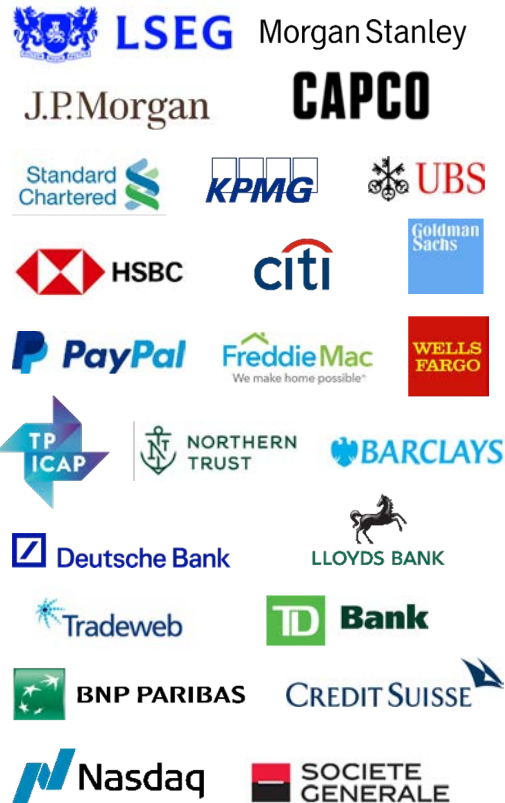


# CDMC: Industry Engagement

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



## CDMC Working Group



## Cloud & Technology Provider Certification



## 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

### 2H 2021 – 1H 2022 Other Industries



- **Life Sciences**
- **Telecommunications**
- **Manufacturing**
- **Retail / Services**
- **Consumer Tech**
- **Government/Defense**
- **Others**

CDMC Working Group Publication on track for Q3 2021



# CDMC Capabilities: Requirements & Automated Controls

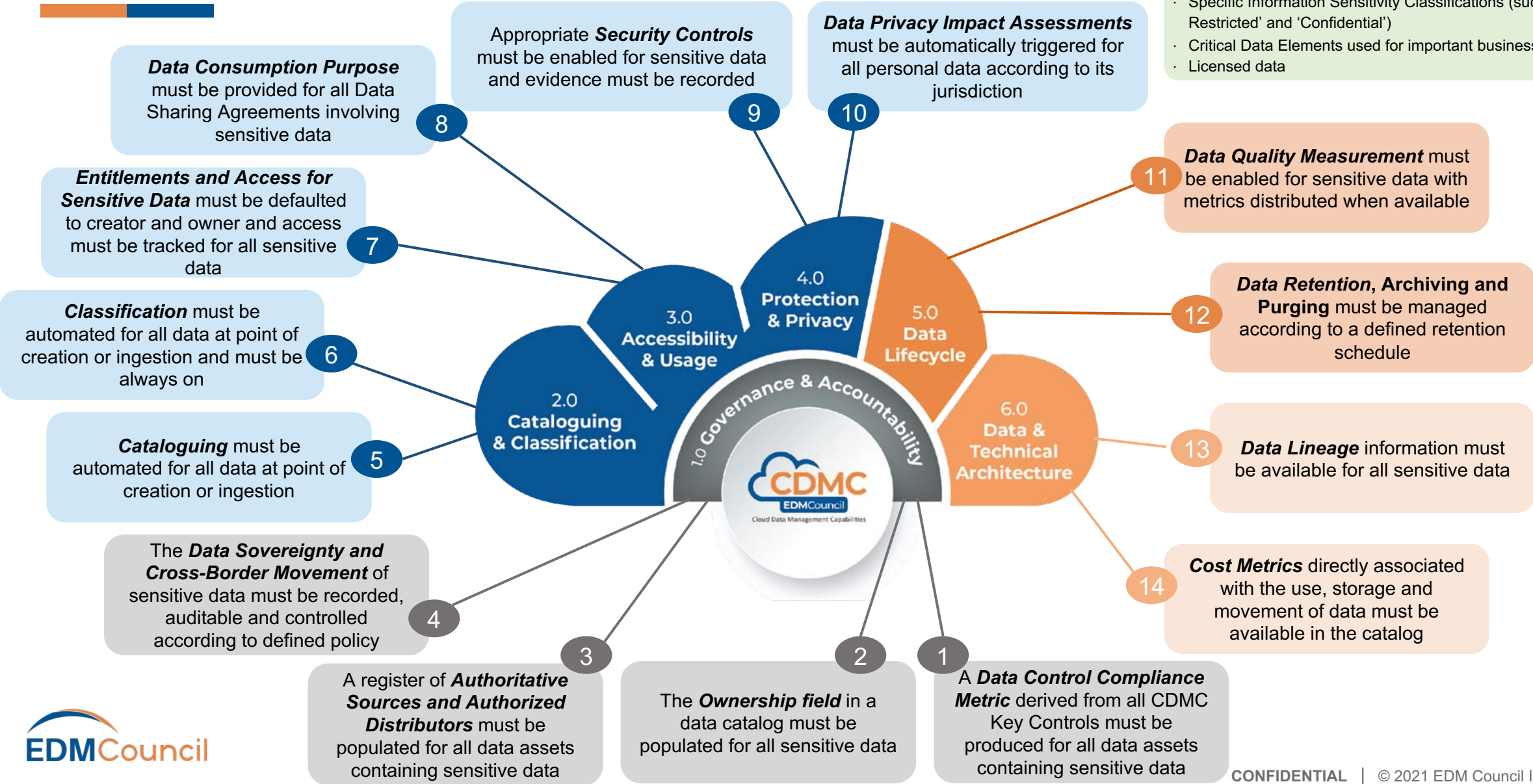
Component	Capability	Sub-Capability	CDMC Automation Checklist (DRAFT)
<b>1. Governance &amp; Accountability</b>	 <b>1.1 The Cloud Data Management business case</b> is defined and measurable	1.1.1 Cloud data management business cases are governed and syndicated 1.1.2 Cloud data management business cases are defined and include a value realization framework	<ul style="list-style-type: none"> <li>Ownership field required for specified classifications (eg PII, MNPI, ISC=HR C)</li> <li>Authorisation field required on cataloged data assets for specified classifications (eg PII, MNPI, ISC=HR C)</li> </ul>
	 <b>1.2 Data ownership</b> established for both migrated & cloud-generated data	1.2.1 Data Owner roles and responsibilities are defined and agreed 1.2.2 Data ownership is established in the Cloud	
	 <b>1.3 Data sourcing and consumption</b> are governed and supported by automation	1.3.1 Data sourcing is managed and authorized 1.3.2 Data consumption is governed and supported by automation	
	 <b>1.4 Data Sovereignty and Cross-Border Data Movement</b> are actively managed	1.4.1 Jurisdictional location of data is tracked and reported 1.4.2 Data Sovereignty and Cross-Border Data movement risks are mitigated	
<b>2. Data Cataloguing &amp; Classification</b>	 <b>2.1 Data catalogues</b> are implemented, used and interoperable	2.1.1 Data cataloguing is defined, scoped and actively used 2.1.2 Metadata is discoverable, enriched, managed and exposed in Data Catalogues 2.1.3 Data catalogues are interoperable across multi and hybrid cloud environments	<ul style="list-style-type: none"> <li>Auto Cataloguing Supported</li> <li>Auto Classification Supported               <ul style="list-style-type: none"> <li>Personal Information auto-discovery</li> <li>ISC auto-discovery (HR C IUO P)</li> <li>MNPI auto-discovery</li> <li>Client Information auto-discovery</li> <li>Additional classifications</li> </ul> </li> </ul>
	 <b>2.2 Data classifications</b> are defined and used	2.2.1 Data classifications are defined and approved 2.2.2 Data classifications are applied and actively used	
<b>3. Accessibility &amp; Usage</b>	 <b>3.1 Data entitlements</b> are managed, enforced and tracked	3.1.1 Data entitlement rights and obligations are captured as metadata 3.1.2 Data entitlement rights are enforced 3.1.3 Enforcement of data entitlement rights is evidenced	<ul style="list-style-type: none"> <li>Entitlements automatically restricted to creator &amp; owner for sensitive data (ISC=HR C IUO)</li> <li>Access tracked for all sensitive data (ISC=HR C IUO)</li> <li>Purpose required for all DSAs for all PII &amp; sensitive data (ISC=HR C IUO)</li> </ul>
	 <b>3.2 Ethical access, use, and outcomes of data</b> are managed	3.2.1 Data Ethics organization structures are established 3.2.2 Data Ethics processes are operational	
<b>4. Protection &amp; Privacy</b>	 <b>4.1 Data is secured,</b> and controls are evidenced	4.1.1 Encryption policies are defined and enforced for data at rest, in motion, and in use 4.1.2 Implementation of data security controls is evidenced 4.1.3 Data obfuscation techniques are defined, scoped and applied 4.1.4 A Data Loss Prevention regime is in place	<ul style="list-style-type: none"> <li>Security controls and DLP are automatically enabled for all sensitive data (ISC=HR C IUO)</li> <li>Security control evidence is sent to Catalog for all sensitive data</li> <li>Recommended data privacy framework workflows (eg jurisdictionally aware PIAs) are automatically triggered for all personal data</li> </ul>
	 <b>4.2 A data privacy</b> framework is defined and operational	4.2.1 A data privacy framework is defined and agreed 4.2.2 The data privacy framework is operational	
<b>5. Data Lifecycle</b>	 <b>5.1 Data quality</b> is managed	5.1.1 Data Quality rules management is established 5.1.2 Data Quality measurement is established and operational 5.1.3 Data Quality metrics reporting is established and operational 5.1.4 Data Quality issue management is established and operational	<ul style="list-style-type: none"> <li>Data Quality metrics information required for specified classifications (eg PII, MNPI, ISC=HR C)</li> <li>Data meeting specific retention schedule classifications is automatically retained, archived and purged</li> </ul>
	 <b>5.2 The data lifecycle</b> is planned and managed	5.2.1 Data archiving and purging are managed 5.2.2 TBA	
<b>6. Data &amp; Technical Architecture</b>	 <b>6.1 Data provenance and lineage</b> are understood	6.1.1 Multi-environment lineage discovery is automated 6.1.2 Data provenance tracking and change management 6.1.3 Data lineage reporting and visualization	<ul style="list-style-type: none"> <li>Provenance information required for specified classifications (eg PII, MNPI, ISC=HR C)</li> <li>Well architected framework evaluated metrics</li> <li>Costs directly associated with managing data assets are available to view by Data Owners in the catalog</li> </ul>
	 <b>6.2 Technical design principles</b> are established and applied	6.2.1 Backups and point-in-time recovery are supported 6.2.2 Optimization of cloud use and cost efficiency is facilitated 6.2.3 Portability & exit planning are supported 6.2.4 Principles for data availability and resilience are established and applied	



# Cloud Data Management Capabilities (CDMC) 14 Key Controls for Managing Data Risk

**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 Regulatory Engagement Update



Cloud Data Management Capability

## Objective

- Engage Global Regulators for CDMC awareness, engagement and feedback

## Key Regulatory Updates

- Formed CDMC Regulatory Engagement Committee
- Significant Momentum in Engaging Regulators

## Completed 3 Initial CDMC Regulatory Briefings

- US Federal Reserve Board
- Bank of England
- APRA (Australia)
- OSFI (Canada)
- ICO (Information Commissions Office UK)

## Upcoming Initial CDMC Regulatory Briefings

- African Regulators (20) Cloud Symposium (July)
- 2nd annual meeting hosted by Standard Bank

## Scheduling CDMC Deeper Dive Sessions

- Bank of England
- Federal Reserve Board (potential OCC addition)
- APRA

## Additional Regulatory Outreach support from EDMC CDMC Partners

- IBM/Promontory, PwC, UBS, Standard Bank, others...

Regulatory Body Outreach	Status	1st Session	Deeper Dive 2nd Session	Next Date	Company	Contacted By
Bank of England	In Progress	Mar 24	Scheduled	Apr 22	IBM Council	J. Bottega
OCC	In Progress	Apr 30	Scheduled	Apr 30	Promontory/IBM	John Asprey
Federal Reserve Board	In Progress	Mar 29	Scheduled	Apr 25	EDM Council	J. Bottega
OSFI (Office of Superintendent of Financial Institutions)	In Progress				EDM Council	J. Bottega
APRA (Australian Prudential Regulatory Authority)	In Progress	Apr 14	Scheduling		PwC	Jim Penson
FCA (Financial Conduct Authority)	In Progress				IBM	S. Mortenson
ESMA (European Securities and Markets Authority)	In Progress				Promontory/IBM	John Asprey
CFTC	In Progress					
Hong Kong Monetary Authority	In Progress			Apr 25	Standard Chartered	Sebastian Wozniowski
Middle East Regulatory Authorities	In Progress			Apr 25	Standard Chartered	Sebastian Wozniowski
African Continent Regulators (20)	In Progress	Apr 11	Scheduled	Jul 13	Standard Bank Group	Sibusiso Ngweni
ICO (Information Commissions Office) UK	In Progress	Apr 30	Scheduled	Apr 30	Promontory/IBM	John Asprey
ECB (European Central Bank)	Follow-up Requested				EDM Council	J. Bottega
BoFin (Federal Financial Supervisory Authority)					Deutsche Bank	John Neesham
MAR (Monetary Authority of Singapore)					IBM Council	J. Bottega
EBA (European Banking Authority)						
NIST (National Institute of Standards and Tech)						
SEC (U.S. Securities and Exchange Commission)					IBM	N/A
Additional US Regulatory Bodies					CBJ	Linda Powell
FINRA (Financial Industry Regulatory Authority)					IBM	N/A
NCUA (National Credit Union Association)						
FinMA (Financial Market Supervisory Authority)	Initial Meeting				UBS	C. Timmers

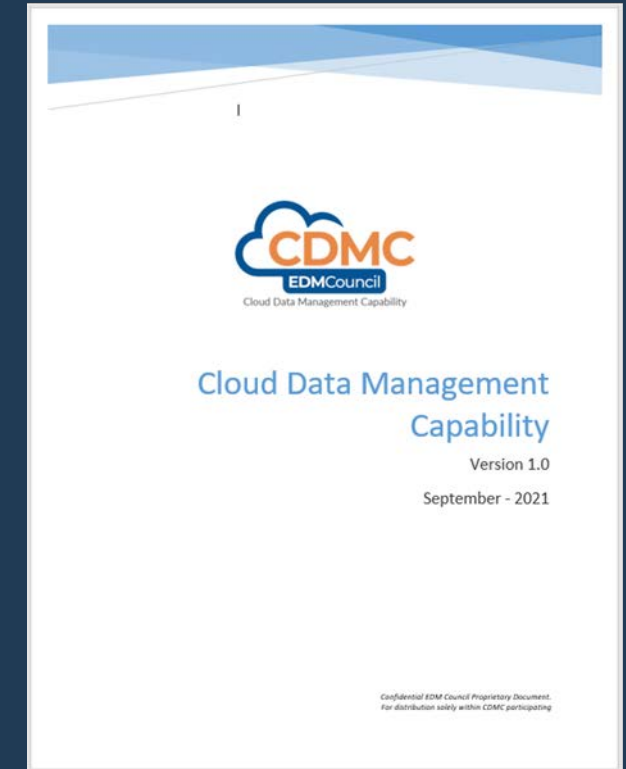
# CDMC Deliverables Availability

- **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>

- **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: Accelerating Trusted Cloud Adoption



## ***CDMC Industry Objective:***

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

## **Companies**

CDMC structured framework of auditable Cloud processes and controls – especially for sensitive data

## **Cloud Service Providers (CSP)**

CDMC requirements and controls can be automated into CSP platforms which accelerates adoption and provides market confidence

## **Application, Technology & Data Providers**

Incorporates certified CDMC capabilities and controls into services and solutions to ensure high degree of reliability and operational effectiveness

## **Consultants & Systems Integrators (SI)**

CDMC enables training & assessments, gap analysis, strategy development, and execution services for end clients adopting cloud

## **Regulators**

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

# Cloud Service Provider Perspective



# Cloud Data Management Capabilities (CDMC) 14 Key Controls for Managing Data Risk

**Sensitive Data** includes classifications such as:

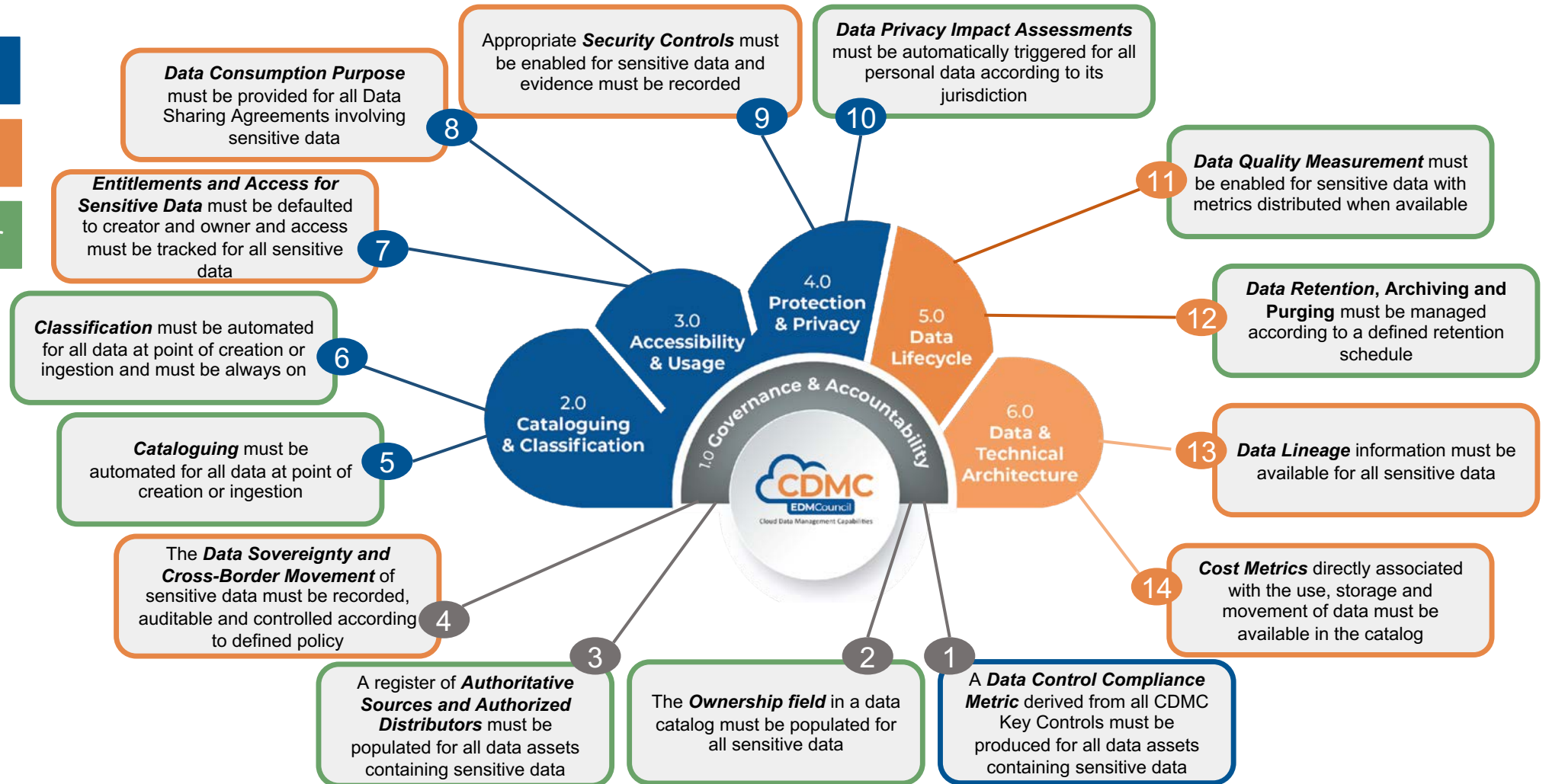
- Personal Information (PI) / Sensitive Personal Data
- Personally Identifiable Information (PII)
- Client Identifiable Information
- Material Non-Public Information (MNPI)
- Specific Information Sensitivity Classifications (such as 'Highly Restricted' and 'Confidential')
- Critical Data Elements used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

## Control Enabled by:

Company + CSP  
+ Tech Provider

Cloud Service  
Provider

Technology Provider



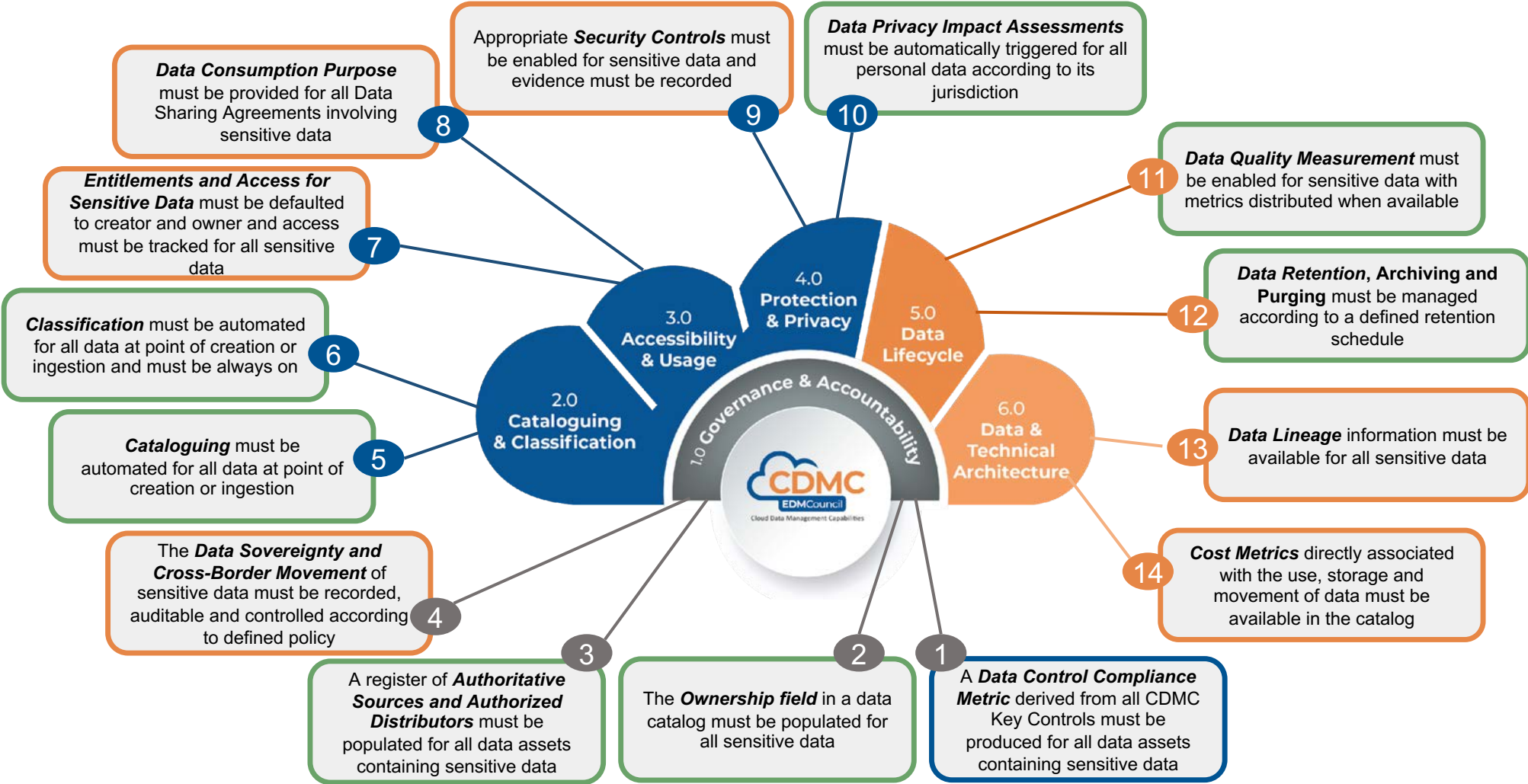
# Technology Vendor Perspective

# Cloud Data Management Capabilities (CDMC)

## 14 Key Controls for Managing Data Risk

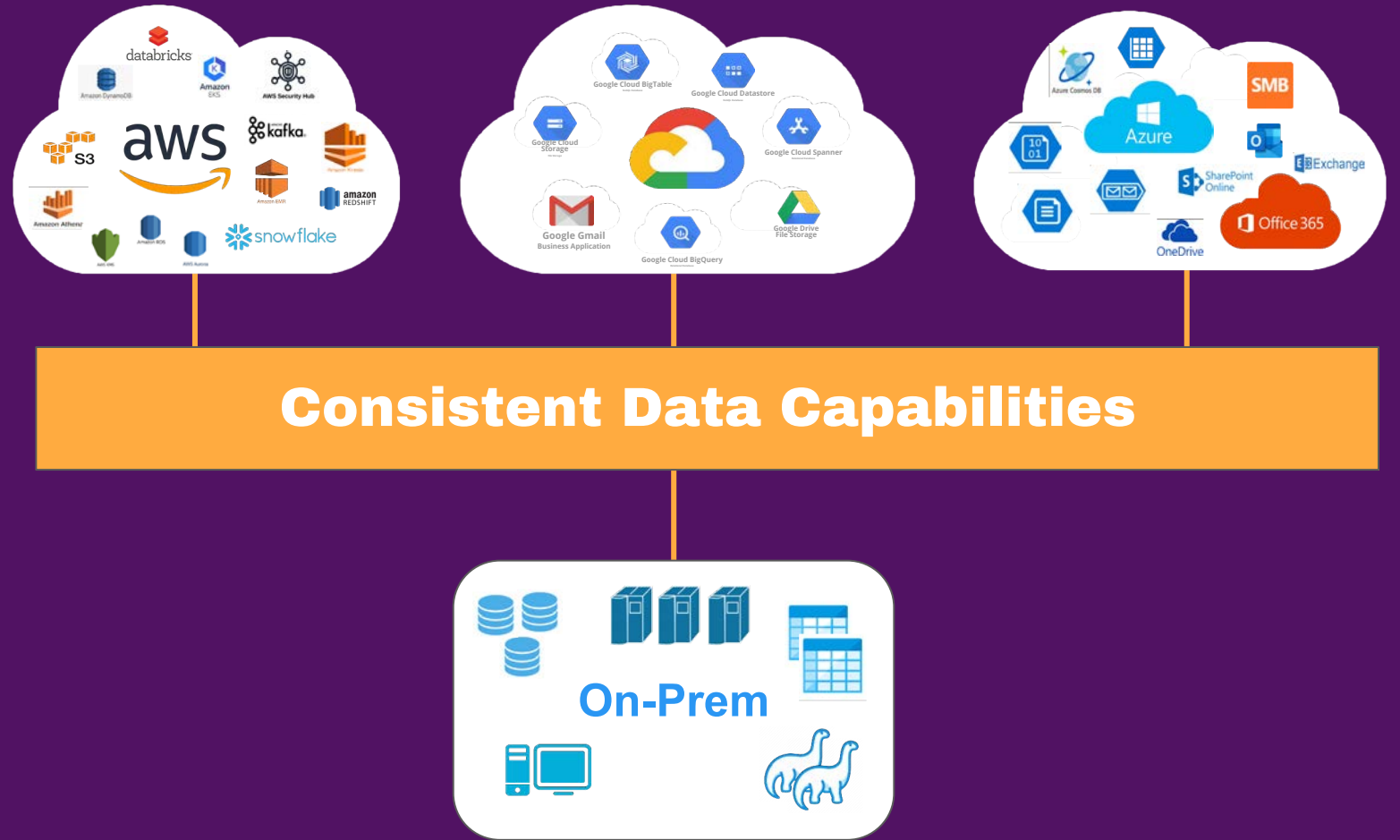
**Control Enabled by:**

- Company + CSP + Tech Provider
- Cloud Service Provider
- Technology Provider



# Creating Consistent Data Capabilities across Environments

- Design for Privacy, Security & Governance
- Must span all clouds
- Enforce consistency
- Minimization principle
- Resilience
- Diverse controls for different actions





# Questions?



**EDM** Webinar 

---

# Data Management Reimagined

Extensible, Open Platform for Data Visibility & Control in Privacy, Security & Governance

Action Your Data



BigID App Marketplace  
for privacy, security,  
and governance controls

Know Your Data



Catalog



Classify



Correlate



Cluster

Discovery-in-Depth for  
deeper data visibility,  
insight, and inventory

Connect Your Data



Files • Images • Unstructured •  
Structured • Big Data • NoSQL •  
Pipeline • SaaS • IaaS • Apps •  
Messaging • Mainframe



**FOR MORE INFORMATION:**

**BigID**

[https://bigid.com/contact/  
info@bigid.com](https://bigid.com/contact/info@bigid.com)

