Innovate Safely in Multicloud with the CDMC Framework for Data Security, Privacy and Governance

A conversation with

Norm Fjeldheim
Former CIO
Illumina and Qualcomm

Amit Bhardwaj
CISO
Lumentum

Oleg Aspis
MD
TIAA

Srinivas Avasarala
VP, Products
SECURITI

EDM Webinar

EDM Council
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)
- Former CEO GoldenSource (2002-2015)
- Former Executive for D&B Software and Oracle
- FinTech Innovation Lab – Executive Mentor (2011 – Present)
Challenges Organizations Face When Adopting Cloud

- Resume
- Credit Report
- Transcript
- Driver's License
- Passport
- Diploma
- Birth Certificate
- Disciplinary Records
- Price List
- NDA
- Invoice
- IRS Form W4
Data Brings Two Big ‘O’s

Data brings

- Immense Opportunities
- Huge Obligations

Data Obligations

- Keep Data Secure from external threats
- Govern For Responsible use of Data
- Use Data respecting global Privacy regulations
- Continuously Comply with 100s of regulations

Data brings

- Obligations
- Opportunities
Cloud Data Management Capabilities (CDMC)

Cloud Challenges

- **Data Risk and Controls**: data, technology, regulatory and planning challenges on every cloud implementation
- **Hybrid / Multi Cloud Environments**: 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 modeled after the DCAM Framework

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

100+ Leading firms and 300+ participants actively participating since May 2020

CDMC Working Group

Cloud & Technology Providers

Regressional Engagement

CDMC Adoption Support

- AWS
- Microsoft Azure
- Google Cloud
- IBM Cloud
- Snowflake
- Collibra
- Informatica
- BigD
- Dataworld
- PRIVITAR
- Securiti

- US: Federal Reserve, SEC, CFTC, FDIC
- Canada: OSFI
- UK: BoE, FCA, ICO
- EU: ECB, ESMA (pending)
- Germany: BaFin
- Switzerland: FinMA
- Australia: APRA
- Singapore: MAS
- Israel: Bank of Israel
- India: RBI, SEBI (pending)
- Africa/Middle East: 20+ Regulators
- Others in process...

CDMC Working Group Delivered release v1.1
28 September 2021

2H 2021 – 1H 2022
Other Industries

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

Other Industries

- J.P. Morgan
- CAPCO
- EY
- Standard Chartered
- HSBC
- Citibank
- KPMG
- UBS
- PayPal
- Freddie Mac
- Wells Fargo
- Lloyds Bank
- Barclays
- DTCC
- Northern Trust
- TD Bank
- Deutsche Bank
- Tradeweb
- BNP Paribas
- Credit Suisse
- Nasdaq
- Societe Generale
Cloud Data Management Capabilities (CDMC)
14 Key Controls for Managing Data Risk

- **Data Control Compliance** must be monitored for all data assets containing sensitive data via metrics and automated notifications.

**Cloud Data Management Capabilities (CDMC)**

**1. Governance & Accountability**
- Data Control Compliance must be monitored for all data assets containing sensitive data via metrics and automated notifications.

**2. Cataloguing & Classification**
- The **Ownership field** in a data catalog must be populated for all sensitive data or otherwise reported to a defined workflow.

**3. Protection & Usage**
- A register of **Authoritative Data Sources and Provisioning Points** must be populated for all data assets containing sensitive data.

**4. Accessibility & Privacy**
- **Data Protection Impact Assessments** must be automatically triggered for all personal data according to its jurisdiction.

**5. Data Lifecycle**
- **Classification** must be automated for all data at the point of creation or ingestion and must be always on.

**6. Data & Technical Architecture**
- **Entitlements and Access for Sensitive Data** must default to creator and owner and access must be tracked for all sensitive data.

**7. Cataloging** must be automated for all data at the point of creation or ingestion, with consistency across all environments.

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

**9. Data Consumption Purpose** must be provided for all Data Sharing Agreements involving sensitive data.

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

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

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

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

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

**Sensitive Data** includes classifications such as:
- Personal Information (PI) / Sensitive Personal Data
- Personally Identifiable Information (PII)
- Personal Health Information (PHI)
- Company or 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

**EDM Council**

Free Download License
Cataloging must be automated for all data at the point of creation or ingestion, with consistency across all environments.
Cataloging

Data Catalogs are Implemented, Used, and Interoperable

Implementation Best Practices

- Automate the discovery of data systems and cataloging of data sets
- Centralize inventory across Multi-cloud, On-prem, SaaS
- Searchable Catalog for both structured & unstructured data
- Open - Integrations with sources to automate sync/exchange via APIs
Classification

Control

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

Auto-discovery

- Personally Identifiable Information
- Information sensitivity classification
- Material Nonpublic Information (MNPI)
- Client identifiable information
- Organization-defined classification
Classification

Data Classifications are Defined and Used

Implementation Best Practices

- Use a consistent detection scheme/grammar for On-premises & Cloud
- Must support structured, semi-structured, and unstructured
- Leverage advanced techniques for higher precision and recall
- Coverage for multi-jurisdiction & languages
- Adopt a single sensitivity level hierarchy and label content accordingly
- Leverage labels for enforcement
Entitlements and Access for Sensitive Data

Control

Entitlements and Access for Sensitive Data must default to creator and owner until explicitly and authoritatively granted.

Access must be tracked for all sensitive data.
Entitlements and Access for Sensitive Data

**Implementation Best Practices**

- Identify and review users and roles that have access to sensitive data & the access paths
- Drive to a least-privilege access model
- Monitor for anomalous access patterns
- Employ dynamic access controls like masking based on roles
- Leverage orchestration tools
Security Controls

Appropriate Security Controls must be enabled for sensitive data.

Security control evidence must be recorded in the data catalog for all sensitive data.
Security Controls

**Implementation Best Practices**

- Use data sensitivity levels to drive protection
- Continuous monitoring and reporting for configuration drifts
- Leverage auto-remediation using cloud APIs
- Automate dynamic data masking policies based on roles and data sensitivity

---

**Data Security**

<table>
<thead>
<tr>
<th>PD</th>
<th>RISK</th>
<th>RESTRICT</th>
<th>ENCRYPT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Moderate</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>Credit Card</td>
<td>Very High</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>SSN</td>
<td>Very High</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>First Name</td>
<td>Moderate</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>Last Name</td>
<td>Moderate</td>
<td>Off</td>
<td>On</td>
</tr>
</tbody>
</table>
Data Sovereignty and Cross-border Transfers

Control

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

Implementation Best Practices

- Along with **Location**, extract the **Residencies** from a data system; Use as basis for jurisdictional requirements
- Build Data Maps to record location of **downstream systems** (incl. sub-processors)
- **Auto-trigger** Transfer Impact Assessments
- Use Residency to **right-size notifications** for Incidents/Breaches
Data Protection Impact Assessments (DPIAs) must be automatically triggered for all personal data according to its jurisdiction.
## Data Protection Impact Assessments

**Implementation Best Practices**

- Extract the **Residencies** from a data system
- Determine the **applicable jurisdictions** for a data system
- Determine the **PII** in the system
- **Auto-Trigger DPIAs** based on applicable jurisdictions and the categories of PII
- Track any gaps discovered in a **Risk Register** for triaging
Questions?

securiti

EDM Webinar
<table>
<thead>
<tr>
<th>Component</th>
<th>Capability</th>
<th>Sub-Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Governance &amp; Accountability</td>
<td>1.1 Cloud Data Management business cases are defined and governed</td>
<td>1.1.1 Cloud data management business cases are defined</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.1.2 Cloud data management business cases are syndicated and governed</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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.2.2 Data ownership is established in the Cloud</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>
</tr>
<tr>
<td></td>
<td></td>
<td>1.3.2 Data consumption is governed and supported by automation</td>
</tr>
<tr>
<td></td>
<td>1.4 Data Sovereignty and Cross-Border Data Movement are managed</td>
<td>1.4.1 Sovereignty of data is tracked</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.4.2 Data Sovereignty and Cross-Border Data movement risks are managed</td>
</tr>
<tr>
<td>2. Cataloguing &amp; Classification</td>
<td>2.1 Data catalogs are implemented, used and interoperable</td>
<td>2.1.1 Data cataloguing is defined, scoped and actively used</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.1.2 Metadata is discoverable, enriched, managed and exposed in Data Catalogues</td>
</tr>
<tr>
<td></td>
<td>2.2 Data classifications are defined and used</td>
<td>2.2.1 Data classifications are defined</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.2.2 Data classifications are applied and used</td>
</tr>
<tr>
<td>3. Accessibility &amp; Usage</td>
<td>3.1 Data entitlements are managed, enforced and tracked</td>
<td>3.1.1 Data entitlement rights and obligations are captured as metadata</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.1.2 Data entitlement rights are enforced</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.1.3 Access and entitlement tracking is automated</td>
</tr>
<tr>
<td></td>
<td>3.2 Ethical access, use, and outcomes of data are managed</td>
<td>3.2.1 Data Ethics organization structures are established</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.2.2 Data Ethics processes are operational</td>
</tr>
<tr>
<td>4. Protection &amp; Privacy</td>
<td>4.1 Data is secured, and controls are evidenced</td>
<td>4.1.1 Encryption policies are defined and enforced</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.1.2 Implementation of data security controls is evidenced</td>
</tr>
<tr>
<td></td>
<td>4.2 A data privacy framework is defined and operational</td>
<td>4.1.3 Data obfuscation techniques are defined and applied</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.1.4 A Data Loss Prevention program is established</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.2.1 A data privacy framework is defined</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.2.2 The data privacy framework is operational</td>
</tr>
<tr>
<td>5. Data Lifecycle</td>
<td>5.1 The data lifecycle is planned and managed</td>
<td>5.1.1 A data lifecycle management framework is defined</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.1.2 The data lifecycle is implemented and managed</td>
</tr>
<tr>
<td></td>
<td>5.2 Data quality is managed</td>
<td>5.2.1 Data quality rules are managed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.2.2 Data quality is measured</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.2.3 Data quality metrics are reported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.2.4 Data quality issues are managed</td>
</tr>
<tr>
<td>6. Data &amp; Technical Architecture</td>
<td>6.1 Technical design principles are established and applied</td>
<td>6.1.1 Optimization of cloud use and cost efficiency is facilitated</td>
</tr>
<tr>
<td></td>
<td>6.2 Data provenance and lineage are understood</td>
<td>6.1.2 Principles for data availability and resilience are established and applied</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.1.3 Backups and point-in-time recovery are supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.1.4 Portability and exit planning are established</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.2.1 Multi-environment lineage discovery is automated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.2.2 Data lineage changes are tracked and managed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.2.3 Data lineage reporting and visualization are implemented</td>
</tr>
</tbody>
</table>
Multiple Deployment Models

**SaaS**
Offered as a SaaS Service from Securiti SaaS Cloud

**Hybrid**
Management & Reporting in Securiti SaaS Cloud. Scanning in Private Accounts using Securiti ElastiPods

**Sovereign**
Entire Offering in Customer’s air-gapped environments
Additional Resources

Cloud Data Management Capabilities (CDMC™) Assessments
Get Started

AI Powered Data Securiti & Privacy across Multi-Cloud, SaaS and On-Premise
Request demo

BLOG
Sensitive Data Intelligence Driven Privacy and Protection

WHITEPAPER
Secure Cloud Data Migration
Download Now
Download CDMC

CDMC Published – Tuesday, Sept 28th
CDMC released as a Free License for Industry

Available for download from EDMC website for internal use for any company
https://edmecouncil.org/page/CDMC

1200+ Global Downloads in 1st week
FOR MORE INFORMATION:

Srinivas Avasarala  
VP Products  
Securiti  

srinivas.avasarala@securiti.ai  
www.securiti.ai