# EDM Webinar 🖭







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







### A conversation with



**Fjeldheim** Former CIO Illumina and Qualcomm





**Oleg Aspis** MD TIAA



Srinivas Avasarala VP, Products SECURITI











# 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













Mike Meriton Co-Founder & COO EDM Council Norm Fjeldheim Ex-CIO Illumina & Qualcomm Amit Bhardwaj CISO Lumentum Oleg Aspis Managing Director-Office of the Chief Data Officer, TIAA Srinivas Avasarala VP Products Securiti

🖸 securiti

EDMCouncil

illumina

LUMENTUM



# Challenges Organizations Face When Adopting Cloud



# Data Brings Two Big 'O's



**Securiti** Confidential Presentation Under NDA - Do Not Distribute - No Screenshots Pls

## **Cloud Data Management Capabilities (CDMC)**

### **CDMC Working Group**



### **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\*



ouncil

### **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





Cloud Data Management Capabilities

### **CDMC: Industry Engagement**

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





ouncil



### Regulatory Engagement C

### EDMCouncil

- 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





- 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



# Cataloging

Control



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

**Securiti** Confidential Presentation Under NDA - Do Not Distribute - No Screenshots Pls

# Cataloging

### Data Catalogs are Implemented, Used, and Interoperable



# 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)

C		
- Г	0	
ι	0	ļ

Client identifiable information



Organization-defined classification

# Classification

### Data Classifications are Defined and Used

#### **Implementation Best Practices**



securit Confidential Presentation Under NDA - Do Not Distribute - No Screenshots Pls

### **Entitlements and Access for Sensitive Data**





م ۹ ۵ ۵ ۵ ۰ ۵ ۲ ۵

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.

Confidential Presentation Under NDA - Do Not Distribute - No Screenshots Pls

### **Entitlements and Access for Sensitive Data**



**Securiti** Confidential Presentation Under NDA - Do Not Distribute - No Screenshots Pls

# **Security Controls**

Control





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

**Securiti** Confidential Presentation Under NDA - Do Not Distribute - No Screenshots Pls

# **Security Controls**



Data Security PD RISK RESTRICT ENCRYPT Moderate Email Very High Credit Card SSN Very High Moderate First Name A Last Name Moderate

### 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**

Control



**Data Protection Impact Assessments (DPIAs)** must be automatically triggered for all personal data according to its jurisdiction.

Confidential Presentation Under NDA - Do Not Distribute - No Screenshots Pls

## **Data Protection Impact Assessments**



# Questions?



# EDM Webinar 🖭

### Securiti Platform

0



### **CDMC** Components, Capabilities & Sub-Capabilities



Component	Capability	Sub-Capability
DE	1.1 Cloud Data Management business cases are defined and governed	1.1.1         Cloud data management business cases are defined           1.1.2         Cloud data management business cases are syndicated and governee
1. Governance	<b>1.2 Data ownership</b> established for both migrated & cloud-generated	1.2.1 Data Owner roles and responsibilities are defined 1.2.2 Data ownership is established in the Cloud
& Accountability	1.3 Data sourcing and consumption     are governed and supported by automation	<ul><li>1.3.1 Data sourcing is managed and authorized</li><li>1.3.2 Data consumption is governed and supported by automation</li></ul>
P	1.4 Data Sovereignty and Cross-Border Data Movement     are managed	<ul><li>1.4.1 Sovereignty of data is tracked</li><li>1.4.2 Data Sovereignty and Cross-Border Data movement risks are manage</li></ul>
2. Cataloguing & Classification	2.1 Data catalogs     are implemented, used and interoperable      2.2 Data classifications     are defined and used	<ul> <li>2.1.1 Data cataloguing is defined, scoped and actively used</li> <li>2.1.2 Metadata is discoverable, enriched, managed and exposed in Data C</li> <li>2.1.3 Data catalogs are interoperable across multi and hybrid cloud enviro</li> <li>2.2.1 Data classifications are defined</li> <li>2.2.2 Data classifications are applied and used</li> </ul>
3. Accessibility	3.1 Data entitlements 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 Access and entitlement tracking is automated
& Usage	3.2 Ethical access, use, and outcomes of data are managed	<ul><li>3.2.1 Data Ethics organization structures are established</li><li>3.2.2 Data Ethics processes are operational</li></ul>
4. Protection & Privacy	4.1 Data is secured, and controls are evidenced	<ul> <li>4.1.1 Encryption policies are defined and enforced</li> <li>4.1.2 Implementation of data security controls is evidenced</li> <li>4.1.3 Data obfuscation techniques are defined and applied</li> <li>4.1.4 A Data Loss Prevention program is established</li> </ul>
(	4.2 A data privacy framework is defined and operational	<ul><li>4.2.1 A data privacy framework is defined</li><li>4.2.2 The data privacy framework is operational</li></ul>
	5.1 The data lifecycle is planned and managed	5.1.1         A data lifecycle management framework is defined           5.1.2         The data lifecycle is implemented and managed
5. Data Lifecycle	5.2 Data quality is managed	5.2.1 Data quality rules are managed 5.2.2 Data quality is measured 5.2.3 Data quality metrics are reported 5.2.4 Data quality issues are managed
6. Data & Technical	<b>6.1 Technical design principles</b> are established and applied	6.1.1 Optimization of cloud use and cost efficiency is facilitated 6.1.2 Principles for data availability and resilience are established and app 6.1.3 Backups and point-intime recovery are supported 6.1.4 Portability and exit planning are established
Architecture	6.2 Data provenance and lineage are understood	<ul><li>b.2.1 Multi-environment lineage discovery is automated</li><li>b.2.2 Data lineage changes are tracked and managed</li><li>b.2.3 Data lineage reporting and visualization are implemented</li></ul>

### Multiple Deployment Models

0



© Securiti Confidential Presentation Under NDA—Do Not Distribute - No Screenshots

# **Additional Resources**



### **Download CDMC**





### CDMC Published – Tuesday, Sept 28th CDMC released as a <u>Free License</u> for Industry

Available for download from EDMC website for internal use for any company

https://edmcouncil.org/page/CDMC











# FOR MORE INFORMATION:

Srinivas Avasarala VP Products Securiti <u>srinivas.avasarala@securiti.ai</u> www.securiti.ai















