EDM Webinar

# Mitigating Generative AI Risks:
## A Framework for Responsible Deployment

*A conversation with*

**Rahul Singhal**
**CPO**
**Innodata**

**David Nadeau**
**VP of Data Science**
**Innodata**

**Heather Frase**
**Lead Scientist**
**ML Commons**

Innodata

ML Commons

EDM Council

# Moderated by **Mike Meriton**
# Co-Founder, 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)
- EDM Council COO (2020-2023)

EDMCouncil

# Today’s panel

Moderator

**Mike Meriton**
Co-Founder
**EDM Council**

**Rahul Singhal**
CPO
**Innodata**

**David Nadeau**
VP of Data Science
**Innodata**

**Heather Frase**
Lead Scientist
**MLCommons**

Innodata

# Security

How are organizations safeguarding data?

# MIT Framework

A comprehensive living database of
AI risks categorized by their cause and risk domain.

| |
|---|
| 1. Discrimination & Taxonomy |
| 2. Privacy & Security |
| 3. Misinformation |
| 4. Malicious Actors & Misuse |
| 5. Human-Computer Interaction |
| 6. Socioeconomic & Environmental Harms |
| 7. AI System Safety, Failures & Limitations |

# Technology

What tools are being used now?

# MLCommons

## Better AI for Everyone

### Global collaborative engineering community

- Non-profit with 125+ members
- Big Tech, Enterprise, Academics, Non-Profits, and Government

### Builds and operates benchmarks and public datasets

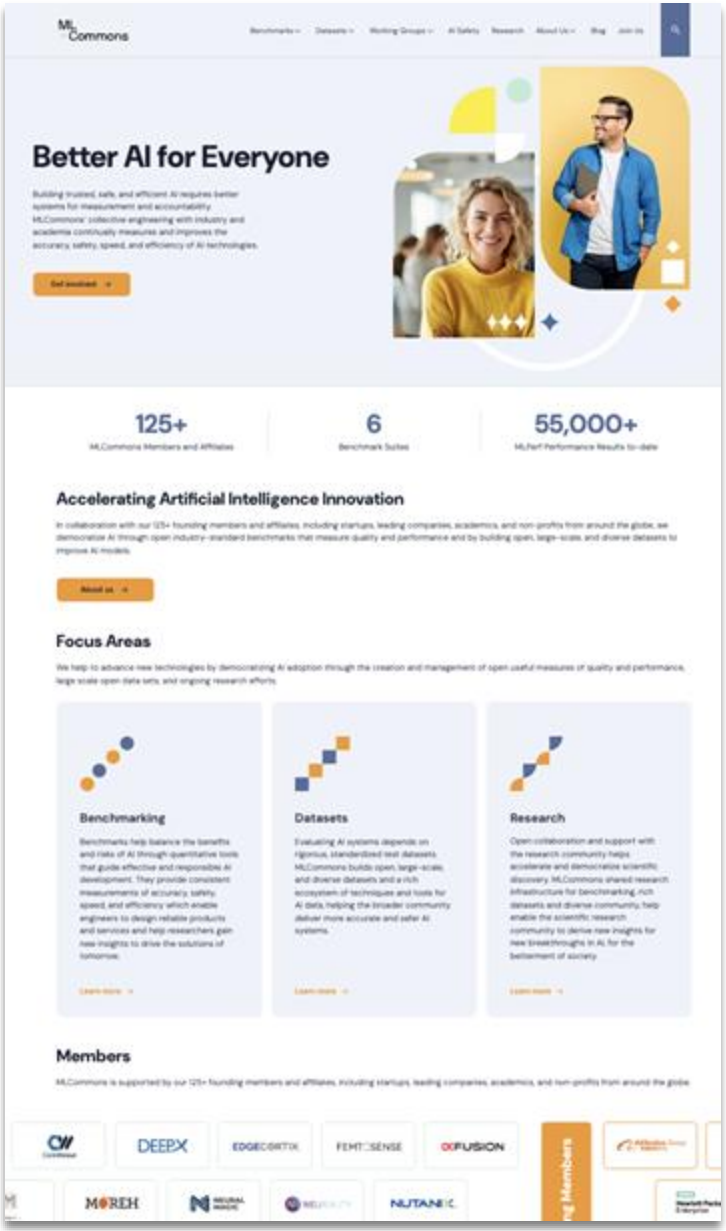
- Our goals: accuracy, efficiency, and safety

### Established in 2020

- The Industry standard for benchmarking AI training/inference speed with 56,000+ MLPerf results to-date

### Measuring AI Risk and Reliability (AIRR) is an new effort

- Developed taxonomy of AI hazards and process for benchmarking generative AI hazards
- Participate in our v1.0 workstreams
- https://mlcommons.org/working-groups/airr/ai-risk-and-reliability/



Better AI for Everyone

Building trusted, safe, and efficient AI requires better systems for measurement and accountability. MLCommons' collective engineering with industry and academia continually measures and improves the accuracy, safety, speed, and efficiency of AI technologies.

Get involved →

125+ MLCommons Members and Affiliates

6 Benchmark Suites

55,000+ MLPerf Performance Results to-date

Accelerating Artificial Intelligence Innovation

In collaboration with our 125+ founding members and affiliates, including startups, leading companies, academics, and non-profits from around the globe, we democratize AI through open industry-standard benchmarks that measure quality and performance and by building open, large-scale, and diverse datasets to improve AI models.

About us →

Focus Areas

We help to advance new technologies by democratizing AI adoption through the creation and management of open useful measures of quality and performance, large scale open data sets, and ongoing research efforts.

Benchmarking

Benchmarks help balance the benefits and risks of AI through quantitative tools that guide effective and responsible AI development. They provide consistent measurements of accuracy, safety, speed, and efficiency which enable engineers to design reliable products and services and help researchers gain new insights to drive the solutions of tomorrow.

Learn more →

Datasets

Evaluating AI systems depends on rigorous, standardized test datasets. MLCommons builds open, large-scale, and diverse datasets and a rich ecosystem of techniques and tools for AI data, helping the broader community deliver more accurate and safer AI systems.

Learn more →

Research

Open collaboration and support with the research community helps accelerate and democratize scientific discovery. MLCommons shared research infrastructure for benchmarking, rich datasets and diverse community help enable the scientific research community to derive new insights for new breakthroughs in AI for the betterment of society.

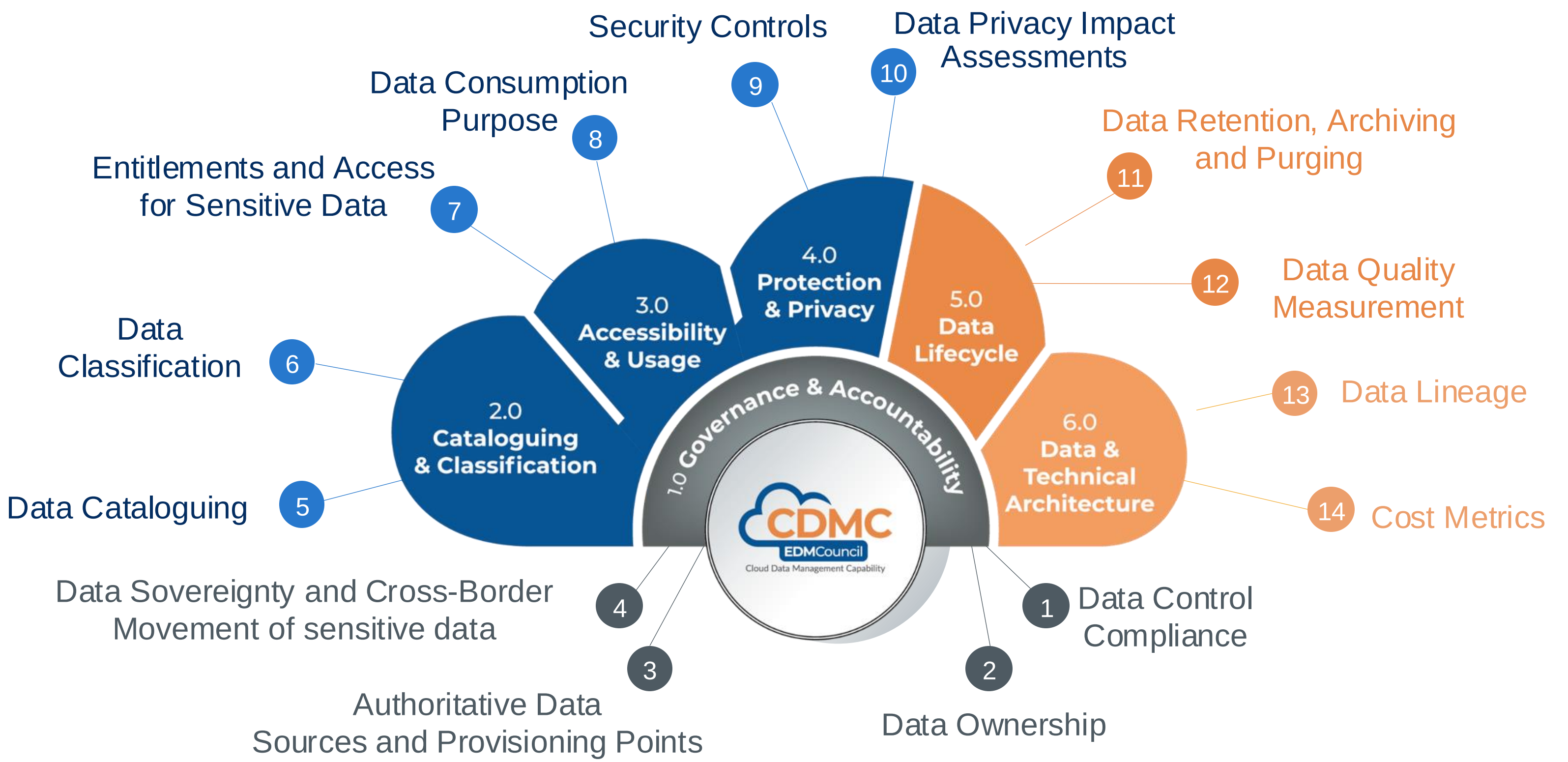
Learn more →

Members

MLCommons is supported by our 125+ founding members and affiliates, including startups, leading companies, academics, and non-profits from around the globe.

# EDM Council – Cloud Data Management Capabilities (CDMC)

## AI Governance – Protecting Sensitive Data in Cloud for AI Initiatives


Security Controls
9
Data Privacy Impact Assessments
10
Data Consumption Purpose
8
Entitlements and Access for Sensitive Data
7
Data Retention, Archiving and Purging
11
4.0 Protection & Privacy
3.0 Accessibility & Usage
5.0 Data Lifecycle
Data Quality Measurement
12
Data Classification
6
2.0 Cataloguing & Classification
1.0 Governance & Accountability
6.0 Data & Technical Architecture
13
Data Lineage
Data Cataloguing
5
CDMC
EDMCouncil
Cloud Data Management Capability
14
Cost Metrics
Data Sovereignty and Cross-Border Movement of sensitive data
4
1
Data Control Compliance
3
2
Authoritative Data Sources and Provisioning Points
Data Ownership

### 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

Microsoft aws Google Cloud

Download CDMC 14 Key Controls: **EDMCouncil.org > Frameworks > CDMC**

# Research

## What’s on the horizon?

# Predictions

Where will be we in 5 years?

# Questions?

Innodata®

ML Commons®

EDM Webinar

# About Us.

A global data engineering company engaged by leading enterprises to help train and deploy cutting-edge AI within their products and operations. Seven of the world's largest tech companies trust Innodata for their AI needs.

**35+**

YEARS

History with a rich legacy as a trusted partner, publicly-traded since 1992.

**5,000+**

GLOBAL EXPERTS

Wide range of subject matter expertise across STEM, finance, healthcare, legal, etc.

**2,300+**

CUSTOMERS

A trusted partner to some of the largest enterprises across the globe, including 5 of the Magnificent Seven.

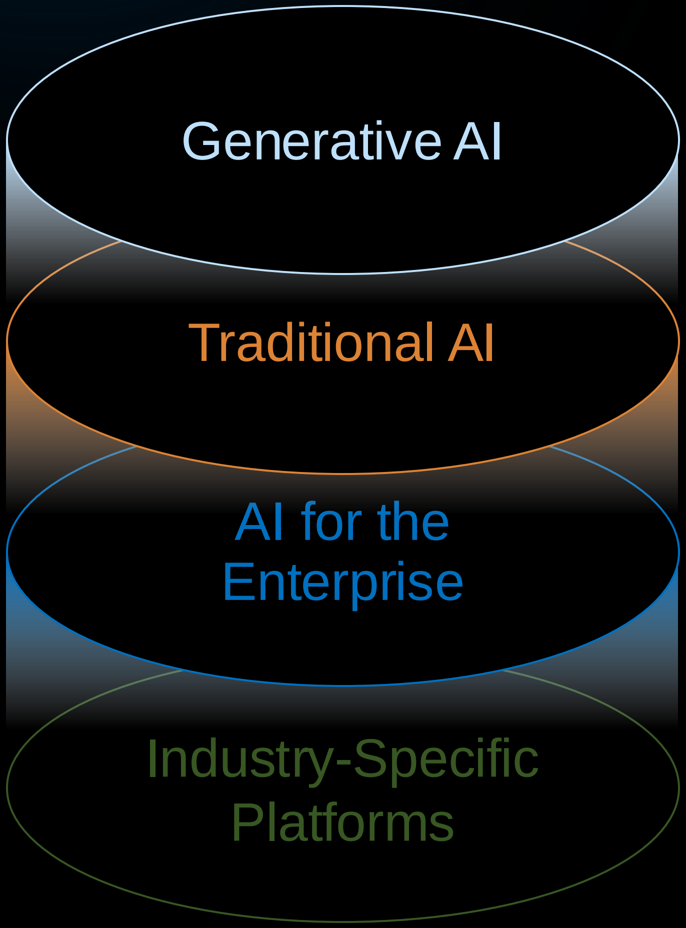
**85+**

LANGUAGES

Ensuring comprehensive language coverage for your projects across 20+ global delivery centers.

Our Services

# End-to-End AI Lifecycle Solutions.



Generative AI

Traditional AI

AI for the Enterprise

Industry-Specific Platforms

Supervised Fine-Tuning

RLHF

Model Safety, Evaluation, + Red Teaming

Data Collection + Creation

GenAI Platform *(Coming Soon)*

---

Data Annotation

Data Collection

Synthetic Data Creation

Annotation Platform

---

Consulting

AI Services

Business Process Management / Managed Services

Digital Services

---

Agility PR

Synodex

# MLCommons

## Better AI for Everyone

### Global collaborative engineering community

- Non-profit with 125+ members
- Big Tech, Enterprise, Academics, Non-Profits, and Government

### Builds and operates benchmarks and public datasets

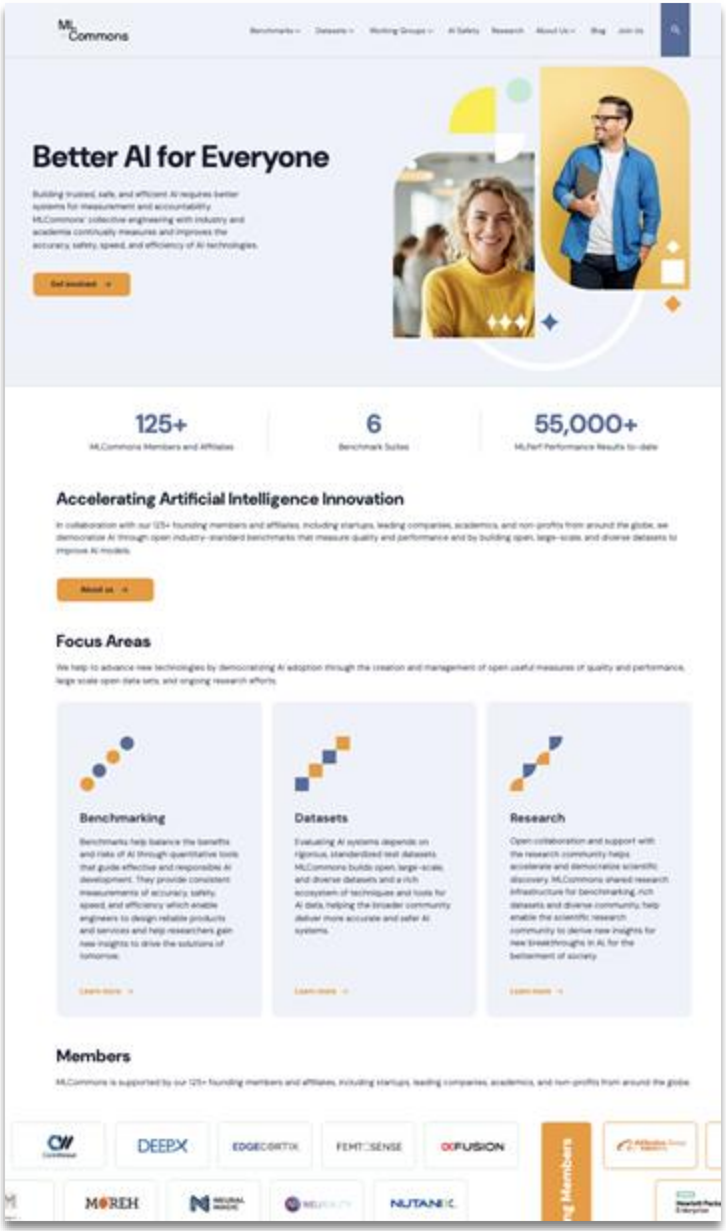
- Our goals: accuracy, efficiency, and safety

### Established in 2020

- The Industry standard for benchmarking AI training/inference speed with 56,000+ MLPerf results to-date

### Measuring AI Risk and Reliability (AIRR) is an new effort

- Developed taxonomy of AI hazards and process for benchmarking generative AI hazards
- Participate in our v1.0 workstreams
- [https://mlcommons.org/working-groups/airr/ai-risk-and-reliability/](https://mlcommons.org/working-groups/airr/ai-risk-and-reliability/)



Better AI for Everyone

Building trusted, safe, and efficient AI requires better systems for measurement and accountability. MLCommons' collective engineering with industry and academia continually measures and improves the accuracy, safety, speed, and efficiency of AI technologies.

125+
MLCommons Members and Affiliates

6
Benchmark Suites

55,000+
MLPerf Performance Results to-date

Accelerating Artificial Intelligence Innovation

In collaboration with our 125+ founding members and affiliates, including startups, leading companies, academics, and non-profits from around the globe, we democratize AI through open industry-standard benchmarks that measure quality and performance and by building open, large-scale, and diverse datasets to improve AI models.

Focus Areas

We help to advance new technologies by democratizing AI adoption through the creation and management of open useful measures of quality and performance, large scale open data sets, and ongoing research efforts.

Benchmarking

Benchmarks help balance the benefits and risks of AI through quantitative tools that guide effective and responsible AI development. They provide consistent measurements of accuracy, safety, speed, and efficiency which enable engineers to design reliable products and services and help researchers gain new insights to drive the solutions of tomorrow.

Datasets

Evaluating AI systems depends on rigorous, standardized test datasets. MLCommons builds open, large-scale, and diverse datasets and a rich ecosystem of techniques and tools for AI data, helping the broader community deliver more accurate and safer AI systems.

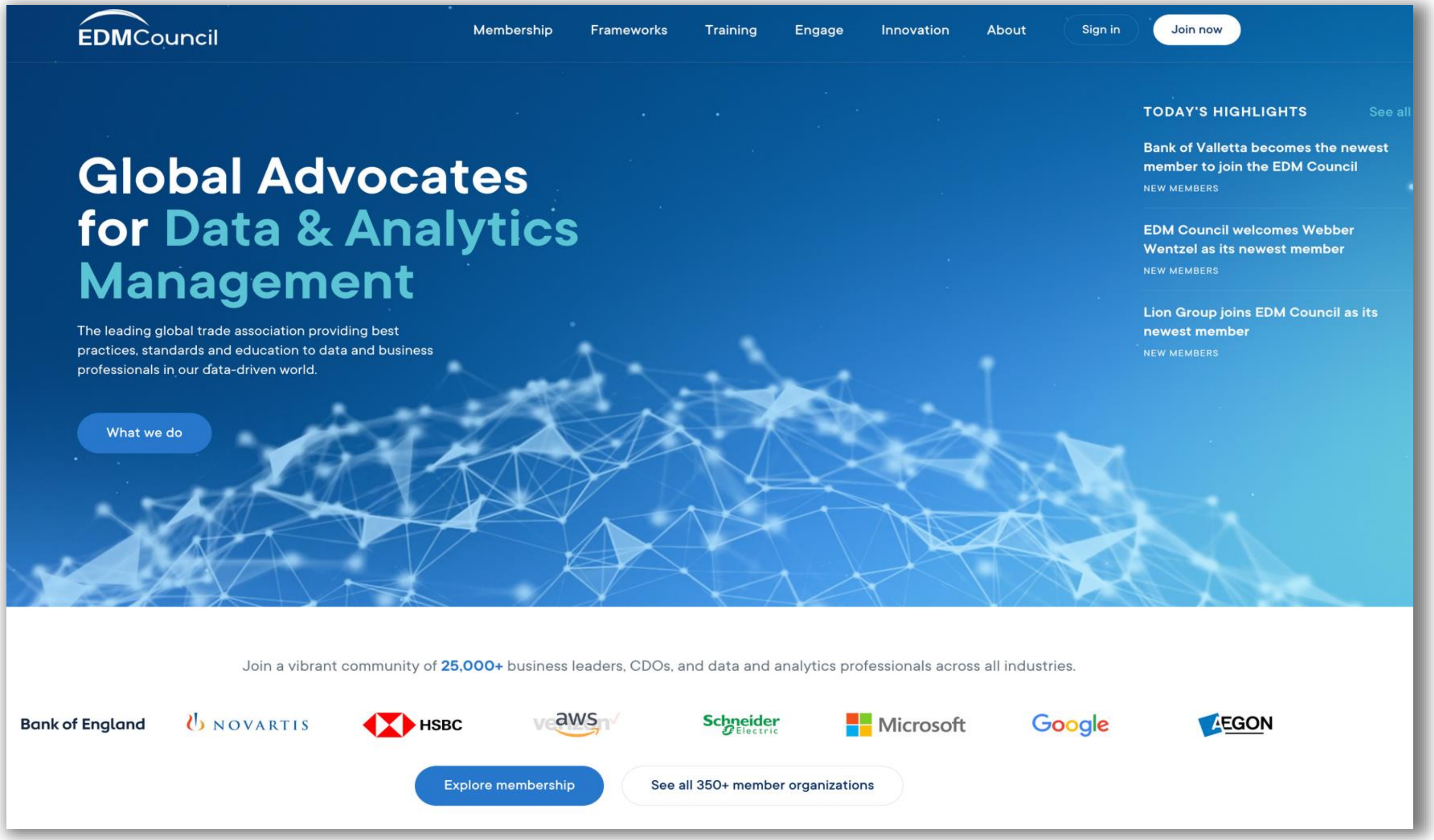
Research

Open collaboration and support with the research community helps accelerate and democratize scientific discovery. MLCommons shared research infrastructure for benchmarking, rich datasets and diverse community, help enable the scientific research community to derive new insights for new breakthroughs in AI, for the betterment of society.

Members

MLCommons is supported by our 125+ founding members and affiliates, including startups, leading companies, academics, and non-profits from around the globe.

# Join EDM Council and our membership community of companies…



## Global Advocates for Data & Analytics Management

The leading global trade association providing best practices, standards and education to data and business professionals in our data-driven world.

TODAY'S HIGHLIGHTS See all

Bank of Valletta becomes the newest member to join the EDM Council
NEW MEMBERS

EDM Council welcomes Webber Wentzel as its newest member
NEW MEMBERS

Lion Group joins EDM Council as its newest member
NEW MEMBERS

Join a vibrant community of **25,000+** business leaders, CDOs, and data and analytics professionals across all industries.

EDMCouncil

**350+ Member Firms**
Cross-industry, including Regulators

**25,000+**
Professionals

**Worldwide**
Americas, Europe, Africa, Asia, Australia

**edmcouncil.org**

DCAM · CDMC EDMCouncil · Data ROI EDMCouncil · ESG EDMCouncil · Open Knowledge Graph INNOVATION LAB · eLearningCurve

EDM Webinar

# Thank you!

**FOR MORE INFORMATION:**

https://Innodata.com
https://mlcommons.org

Innodata®

EDMCouncil