# Invisible Governance Embedding Guardrails Without Slowing Innovation

Emma York
Sanja Hukovic

LSEG

## Emma York

Corporate Chief Data Officer & Head of Enterprise Data Enablement

- Leading Enterprise data management strategy
- Driving data and records by design - governance without friction, trust at source
- Embedding data quality, literacy, culture, and platform-driven automation
- Delivering trusted corporate data, metadata-first thinking, and AI-enabled governance
- Former leadership roles at Morgan Stanley – data and non data!

## Sanja Hukovic

Head of Model and AI Risk Lead

- Enterprise Model & AI Risk lead for LSEG
- Architect of AI governance and control standards
- Specialist in structured products & quantitative validation
- Focused on safe, scalable AI adoption

# Who we are

LSEG

Make more possible

We are a **leading global financial markets infrastructure** and **data provider**.

We play a vital **social** and **economic role** in the world's financial system.

With our trusted expertise and global scale, we enable the **sustainable growth** and **stability of our customers** and their communities.

**300+** Years of experience

**170+** Countries served

**26,000+** Employees

**44,000+** Customers

# We deliver deep expertise globally, across multiple asset classes and across the full trade lifecycle

## Trade Lifecycle

**Serving customers pre/at/post trade**

| Capital Formation & Issuance | | | | Pre-Trade & Liquidity Discovery | | | | Trade Execution | | Post-Trade & Capital Optimisation | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Private placements | Public issuance & issuer services | Fund Development | Investor onboarding | Investment Design & Research | Reference Data & Onboarding | Pre-Trade Data & Analytics | Price & Liquidity Discovery | Trade Execution Workflow | Execution Trading Venues | Clearing (Traditional & "cleared" bilateral) | Settlement & Asset Services | Reporting | Post Trade Data, Analytics & Solutions |
| LONDON STOCK EXCHANGE | FTSE RUSSELL | LSEG RISK INTELLIGENCE | FTSE RUSSELL | LSEG DATA & ANALYTICS | LSEG DATA & ANALYTICS | | | LSEG DATA & ANALYTICS | Tradeweb LSEG FX | LONDON STOCK EXCHANGE | LSEG POST TRADE | LSEG POST TRADE | POST TRADE SOLUTIONS LSEG DATA & ANALYTICS |

## Data value chain

**Serving FS and new customer segments**

| Data Sourcing | | Data Management & Transformation | | Models & Analytics | | Distribution | |
|---|---|---|---|---|---|---|---|
| Data Acquisition | Data Processing | Storage & Management | Customisation & Integration | Models | Analytics | Delivery & Access | Channel |

LSEG | Microsoft

# Invisible Governance: Embedding Guardrails Without Slowing Innovation

## Discussion points

Designing governance frameworks that work for business, not static rulebooks

AI risk management and embedding Responsible AI principles seamlessly

Where data fits: foundations vs opportunities

Our top tips

# Slido

## Are data controls integrated into your AI Governance process

1. Fully
2. Partially
3. Not sufficiently

LSEG

# Designing governance frameworks that work for business, not static rulebooks

LSEG

# Common AI Risks

AI risks exist throughout the AI life cycle and need to be monitored.

Below we give some key risk and how to identify them.

Note that data is the underlying cause of multiple risks such as Bias and Quality below

### Hallucination

Producing confident, plausible answers that are completely or partially false

### Jail breaking

Bypassing safeguards to produce harmful outputs

### Bias

Pre-trained models can encode biases/ hidden preferences that shape the outputs, which can go unnoticed

### Data Risks

Exposure of sensitive information – restricted data may be revealed unintentionally. Misuse of data – data may be processed in ways that breach policy, contractual rights, or regulatory requirements

### Drift

Model performance can change over time as real-world conditions slowly change

### Overconfidence

Users over-trust AI skipping critical thinking and fact checking

### Unintended consequences

Where an agent or system takes actions without sufficient guardrails negatively impact operations

### Quality

Poor-quality results can stem from **weak or outdated data** or model limitations, so always review and validate AI outputs before using them

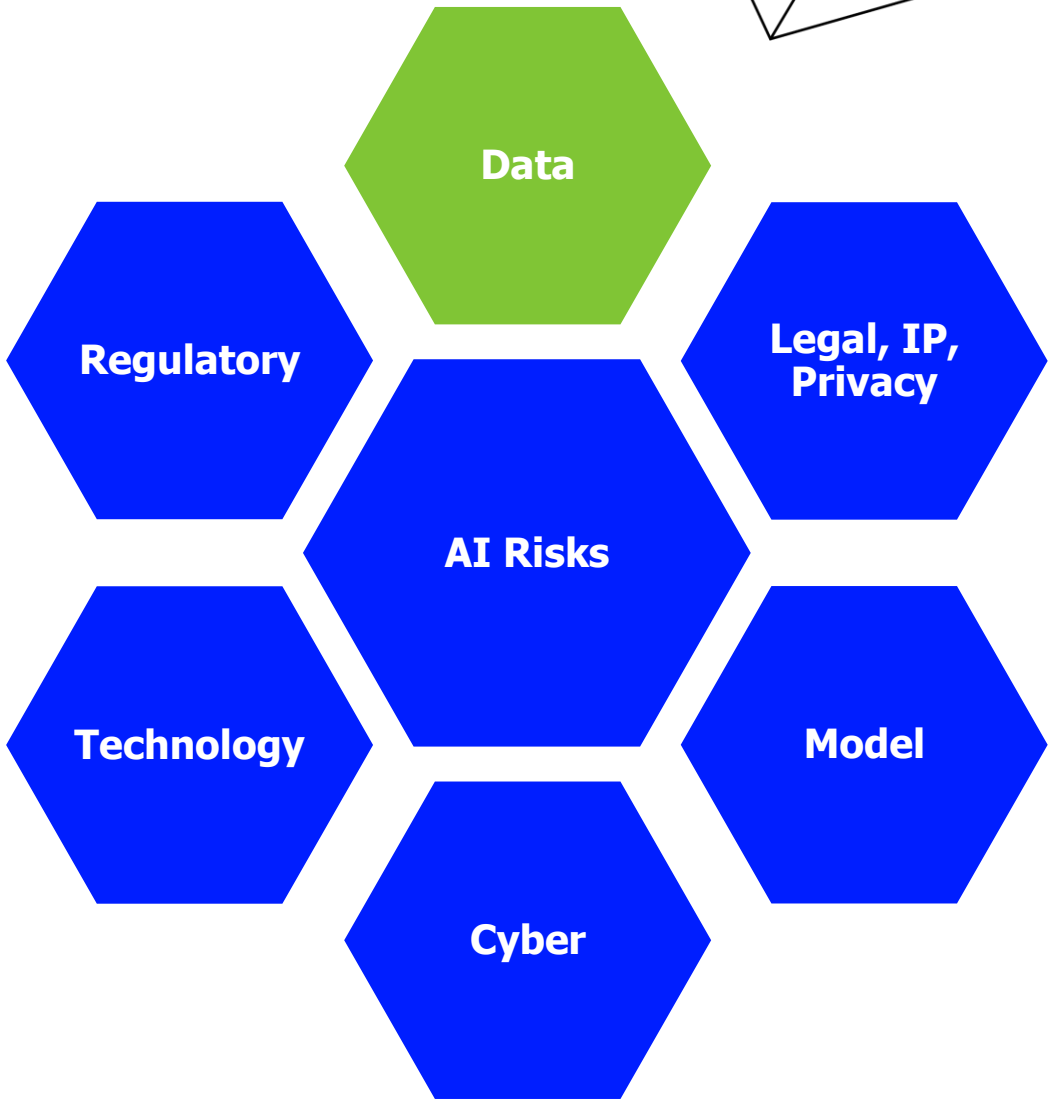
# AI Risk Taxonomy

AI risk management is fully embedded within the LSEG Enterprise-Wide Risk Framework, aligning with existing governance, controls, and reporting structures.

***AI Definition*** *– EU AI Act*

***AI Appetite*** *– Aggregate of constituents or defined across AI pillars*

***AI Principles*** *– LSEG Responsible AI Principles*

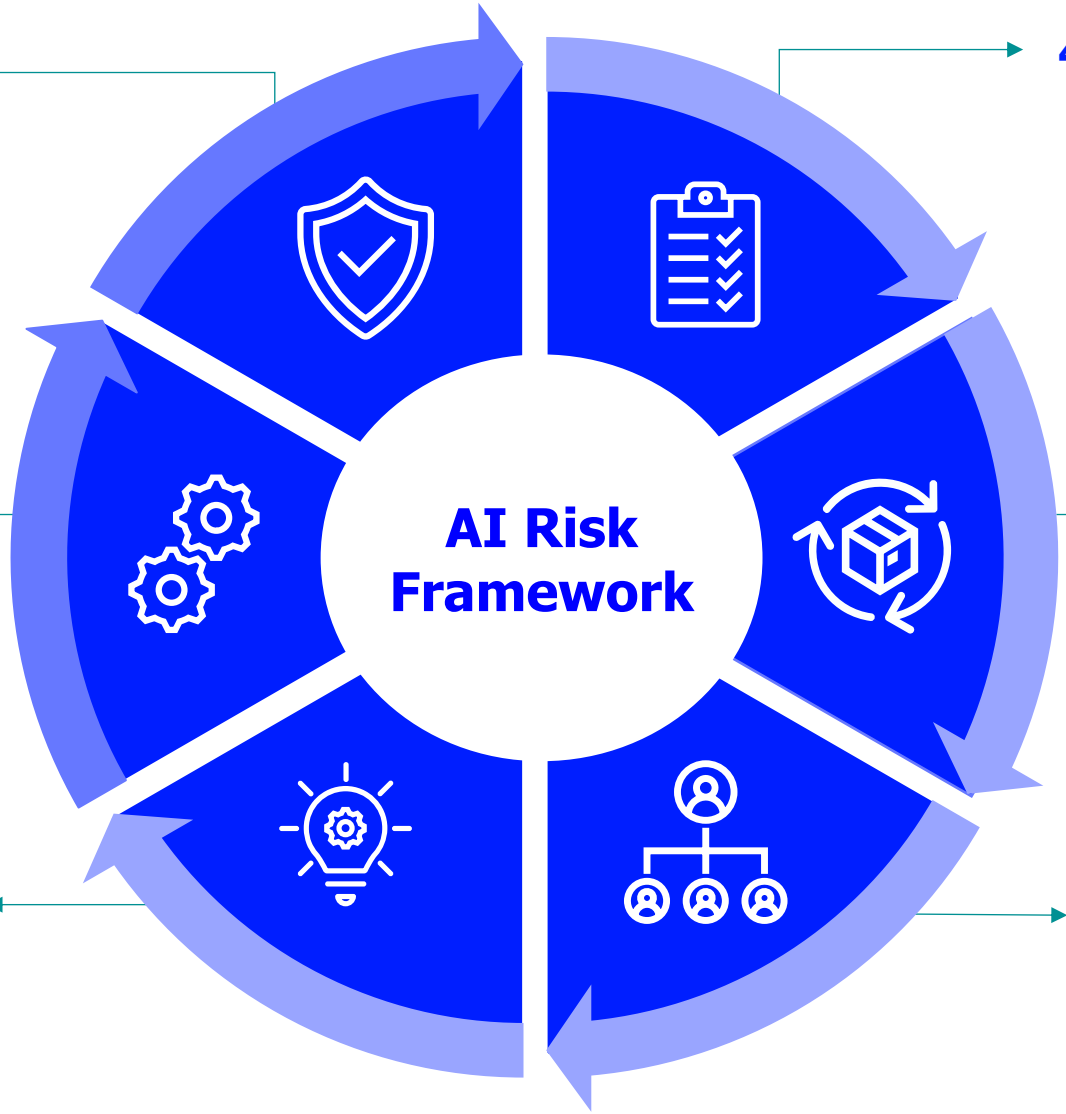


# LSEG AI Risk Management Framework

AI Risk Management Framework establishes key principles and processes for identifying, monitoring, and managing AI-related risks

### 3. AI Flow and Inventory
- Governance Pre-Approval
- Governance Approval
- AI Inventory

### 4. AI Risk and Controls
- AI Risk definition
- AI controls, including data controls
- AI Tier is an extension of model Tier
- AI validation efforts are commensurate with AI Tier




### 2. AI Development
- Experimentation platform
- AI Implementation Guidelines
- AI Literacy and Upskilling

### 5. AI Lifecycle
- AI Use
- AI Monitoring and Incident Response
- AI Change Management and Retirement

### 1. Responsible AI Concepts
- AI Definition
- Responsible AI Principles

### 6. Roles and Responsibilities
- 1LOD: AI use case Owner, AI Developer, AI User
- 2LOD: Risk, Legal and Compliance

# AI risk management and embedding Responsible AI principles seamlessly

LSEG

# LSEG Responsible AI Principles

| | |
|---|---|
| **Accurate and Reliable** | Accuracy and Reliability of AI is demonstrated by the consistent performance or results of AI deployment. The aim of this requirement is to ensure that AI systems perform correctly and dependably, delivering expected results to users. |
| **Accountable and Auditable** | Accountability and Auditability in AI reflect the extent to which information about an AI system is available to individuals. AI systems must have clear governance implemented and flag AI outputs. |
| **Safe** | AI systems must be designed and tested to prevent harm to users and the environment, ensuring their operation does not pose undue risks. This principle involves identifying potential risks and actively working on their mitigation. |
| **Secure and Resilient** | AI systems must be secured against unauthorized access and attacks, with robust measures to ensure their resilience and maintain the integrity of data and operations. AI systems must have protocols in place to avoid, respond to, or protect from attacks. |
| **Interpretable and Explainable** | Interpretability and Explainability in AI involve detailing how the underlying (AI) technology works and how the model reached a given output. This principle focuses on offering users information which will help them understand the functionality, purpose, and potential limitations of an AI system. |
| **Privacy and IP Protected** | AI Systems must prioritise the protection of personal data, ensuring that user privacy is upheld through robust data handling and anonymisation techniques. LSEG respects IP rights in our use of AI and only use content/data that we have the appropriate authorisations for, while also protecting our own content/data. |
| **Fair** | Developers and users of AI should identify and mitigate biases in AI systems, which can otherwise lead to unfair outcomes. This principle focuses on the need to have fair AI systems that align with LSEG's values and culture. |

# AI Validation Framework

| LSEG Responsible AI Principle | Model Risk Assessment Method – data lens |
|---|---|
| **Privacy and IP Protected**<br>**Fair** | Compliance with EU AI Act, **PII data detection** |
| **Accurate & Reliable**<br>**Accountable & Auditable**<br>**Fair** | **Data relevance, accuracy, completeness, toxicity, bias**; sentiment analysis for textual input |
| **Fair** | Toxicity models (e.g. Toxic BERT) or manual evaluation for model **input/output data** |
| **Accurate & Reliable** | SME/gold standard testing, **dataset evaluation**, accuracy metrics, LLM-as-a-judge, hallucination, misleading output, answer transparency |
| **Secure & Resilient**<br>**Safe** | Out-of-domain testing for prompt injection and jailbreak attacks |
| **Accountable & Auditable**<br>**Interpretable & Explainable** | Development documentation and transparency note review |

# Where data fits: foundations vs opportunities

LSEG

# Where data fits: foundations vs opportunities

Does Agentic AI supercharge premise that DG is the non-negotiable foundation for ethical, scalable, and effective AI?

YES

- Unlike traditional AI models, agentic AI operates autonomously.
- With reduced human oversight, robust data governance becomes **imperative** to ensure that AI-driven decisions are **secure, accurate and aligned with ethical standards**
- The same AI agents driving this evolution can also **redefine governance and data risk control, enabling its enforcement at scale**

**2 conclusions:**

**We need to supercharge** Data Governance. It's a prerequisite for AI (Generative and Agentic)

**BUT, we have an opportunity** to use agents to scale Data and Records Governance

# Slido

**Are you primarily *strengthening data foundations* to enable AI or using AI to *create governed assets?***

1. Strengthening data foundations for AI
2. Using AI to create governed assets
3. Doing both equally
4. Not sure / still exploring

**Is your organisation investing more in *AI use cases* or in *data governance* to make AI safe and scalable?**

1. AI use cases
2. Data governance
3. Both equally

LSEG

# Best Practices Framework

## CDMC Builds on EDM Association's Experience Developing and Supporting DCAM – Data Management Capability Assessment Model

### WHO?

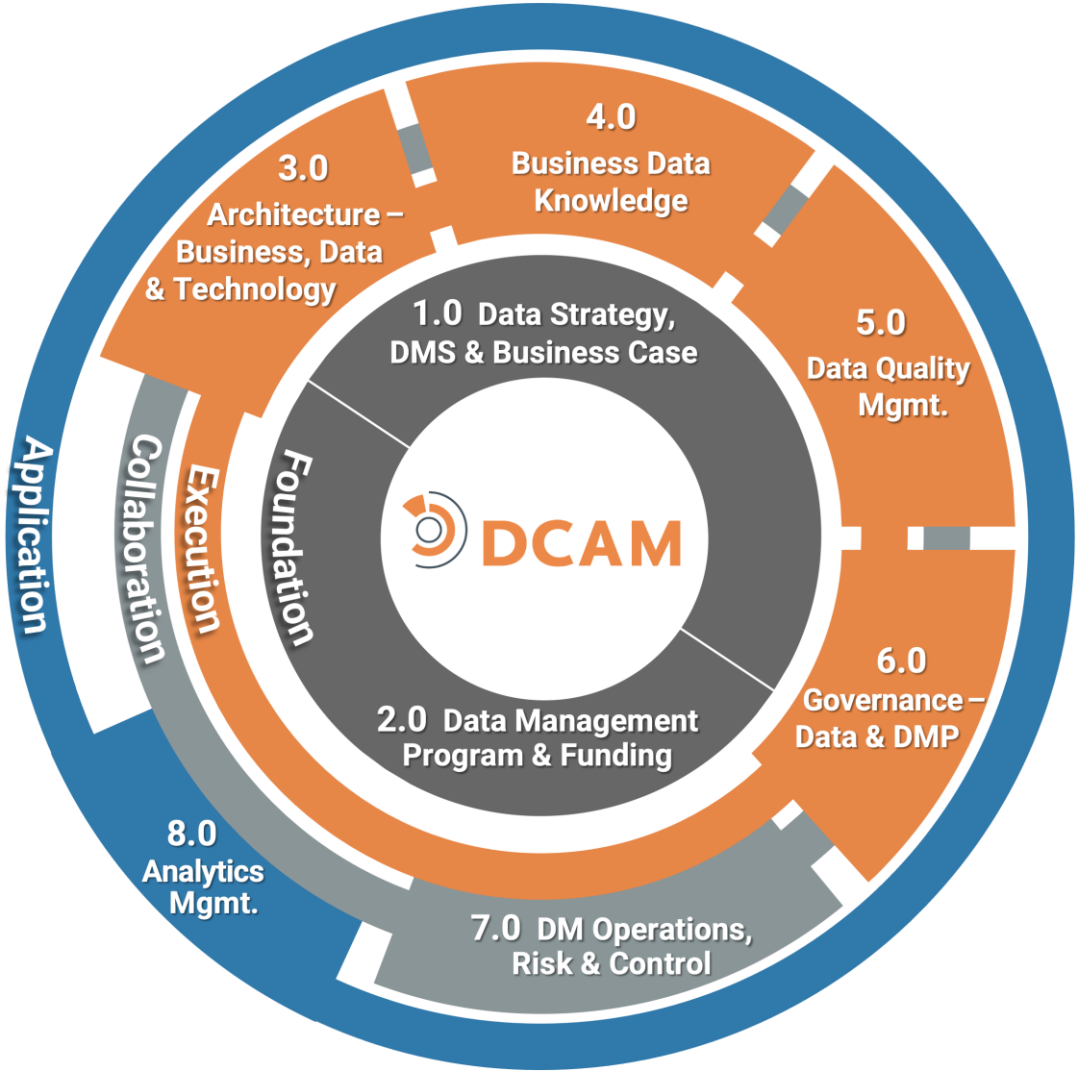
- Developed via member collaboration
- **62%** of Council members using frameworks use DCAM

### WHAT'S IN DCAM?

- 8 components, 34 Capabilities, 101 Sub-capabilities
- Members flexibly apply to their organization
- Includes: Data Supply Chain, Advanced Analytics, Data Ethics and Responsible AI/ML

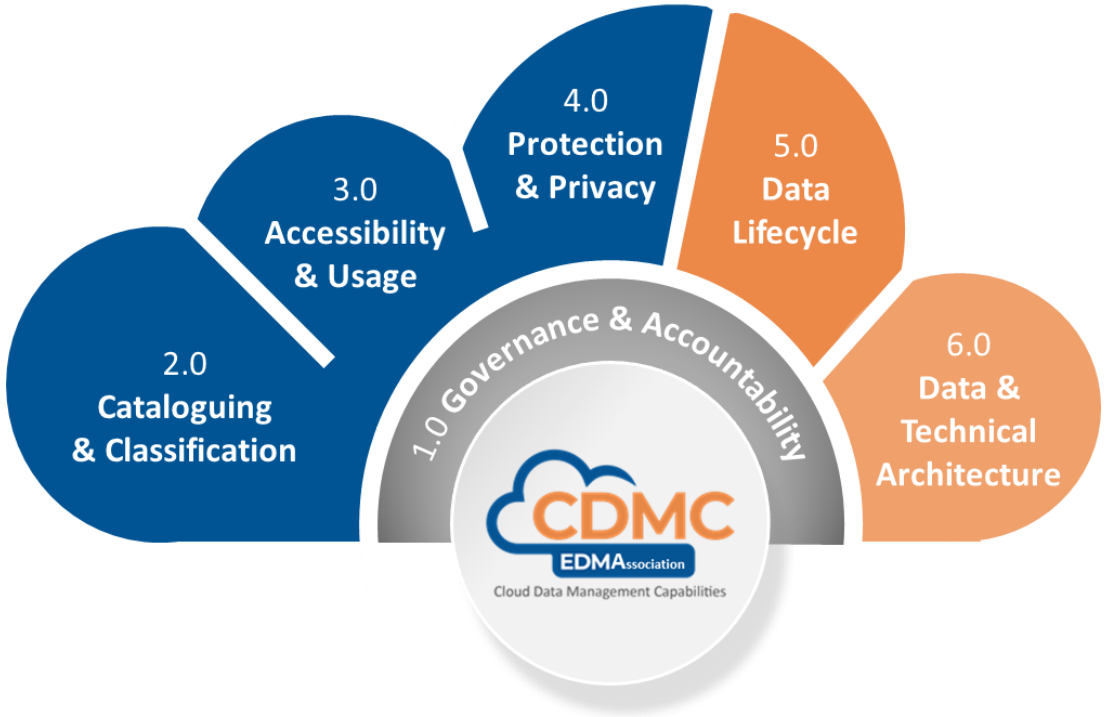
### USED FOR:

- Program Initiation & Funding
- Team Training & Common Language
- Assessments & Benchmarking



A comprehensive specification of Data Management best practice in cloud, multi-cloud and hybrid environments

# CDMC Overview



# Cloud Data Management Capabilities (CDMC) for AI, Data & Analytics Controls (ADAC)

CDMC EDMAssociation
Cloud Data Management Capabilities

## ANALYTICS

**Specialised capabilities to govern & manage analytics & AI use cases**

***USE CASE: Ethical Purpose/Intent, Use* and Outcomes** must be respectively scoped & aligned, disclosed, and governed for all sensitive assets — 8

***ETHICS & PRIVACY IMPACT: Assessments*** must be automatically triggered, or revisited, for personal, group, community & societal outcomes, and data processing (inc indirect or proxy variables), according to its jurisdiction — 10

***PERFORMANCE: Model Quality Controls*** must be enabled, and ongoing, for sensitive assets with metrics distributed alongside assets as applicable (inc bias, drift, consistency) — 15

**RISK:** A ***Risk Control Compliance Metric*** must be produced for all sensitive assets — 1

***AUDIT: Lineage, Transparency, Versioning and Reproducibility*** information must be available for all sensitive assets, including traceability of data & functional lineage, and appropriate model transparency & explainability — 13

## DATA & ANALYTICS

**Common capabilities for managing data & analytics assets**

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

***Cataloguing*** must be automated for all assets (data, models & other artefacts) at point of creation or ingestion — 5

***Entitlements and Access for Sensitive Assets*** must be defaulted to creator and owner, and all access and use must be tracked — 7

***Appropriate Security Controls*** *must be enabled for sensitive assets and evidence must be recorded, inc vulnerability assessment for inputs & outputs* — 9

***Quality Measurement*** must be enabled for sensitive assets with metrics distributed alongside assets as applicable (inc accuracy, completeness, timeliness) — 11

The ***Ownership field*** in a catalog must be populated for all sensitive assets — 2

***Data Sovereignty and Cross-Border Movement*** of sensitive assets must be recorded, auditable and controlled according to defined policy (including data localisation and software export rules) — 4

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

***Retention, Archiving and Purging,*** must be managed according to a defined framework — 12

***Cost & Sustainability Metrics*** directly associated with the compute, storage and movement of assets must be available in the catalog and used to optimise design — 14

## DATA

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

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

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

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

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

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

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

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

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

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

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

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

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

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

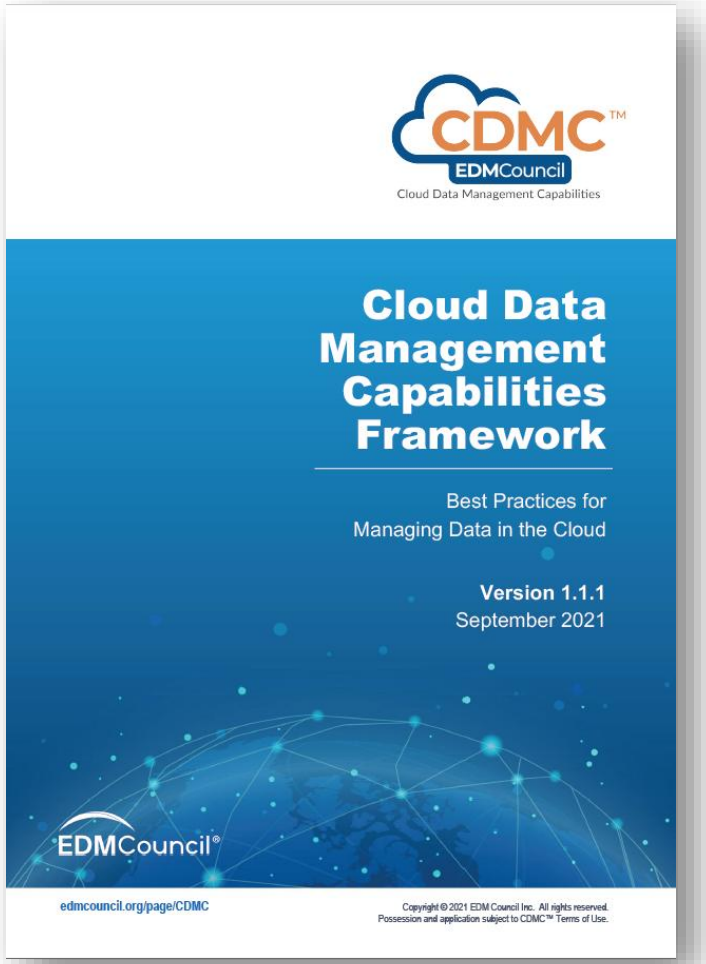
**Classification of Sensitive Assets** includes:

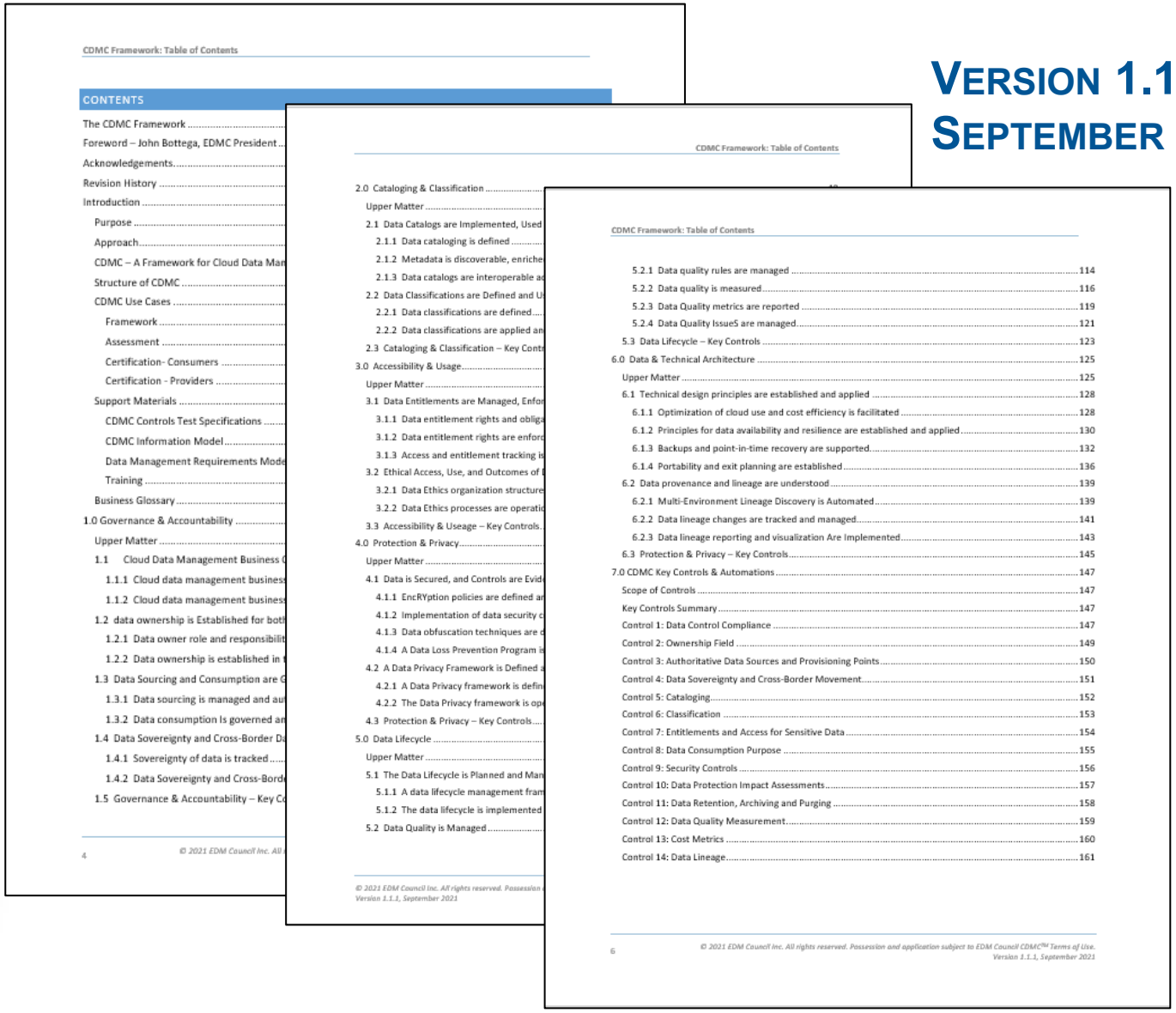
- Personal Information (PI) / Sensitive Personal Data
- Personally Identifiable Information (PII)
- Client Identifiable Information
- Material Non-Public Information (MNPI)
- Specific Information Sensitivity Classifications (such as 'Highly Restricted' and 'Confidential')
- Critical Data Elements used for important business processes
- Licensed data
- Model IP [new]
- EU AI Act High Risk intended use models [new]


LSEG

EDM Association

# CDMC Framework

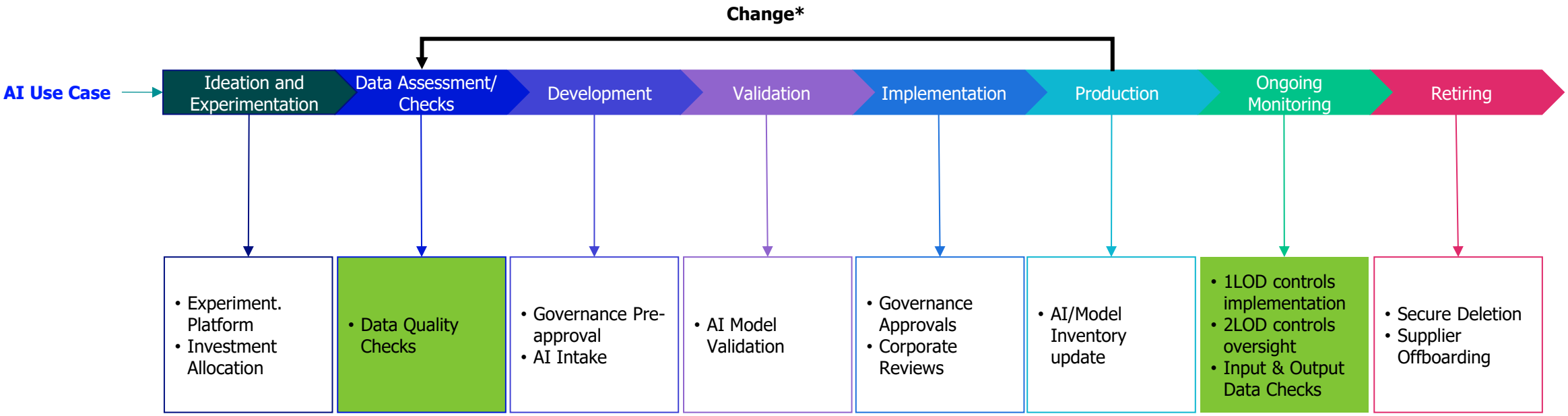



## VERSION 1.1 PUBLISHED SEPTEMBER 2021

# AI Lifecycle

- AI Lifecycle comprises of 8 stages as depicted below.
- *AI model change will trigger a new approval process and can be prompted by:
  - desire to improve methodology
  - changes to the AI usage/expanded scope
  - weakening model performance (e.g., model drift)



# Slido

How far along are you in building Agentic AI governance

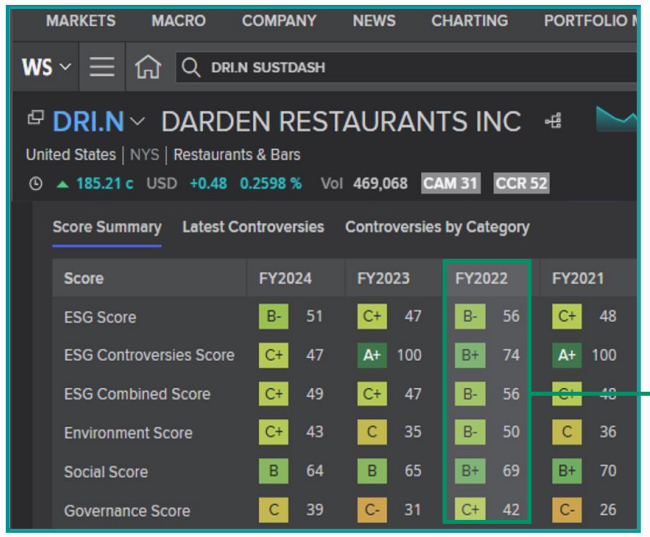
1. Finalized
2. Almost there
3. Not started

LSEG

# LSEG Example

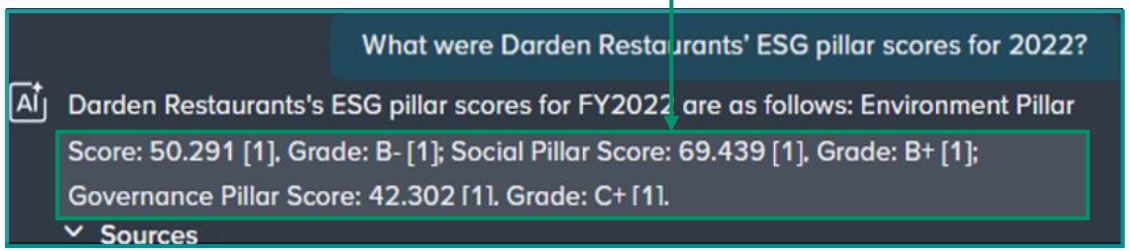
Most enterprise LLM use cases leverage data extraction pipelines to ground model outputs in reliable data sources. LSEG MRM team applies the GenAI Validation Framework to ensure factual accuracy, robustness, and regulatory compliance across these models.

## Numerical data

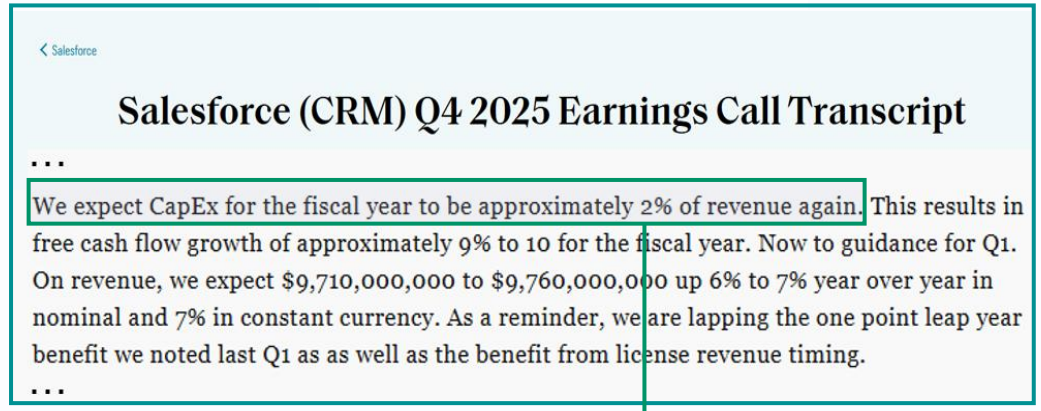



**API** systems extract **numerical data** from various LSEG databases, such as:

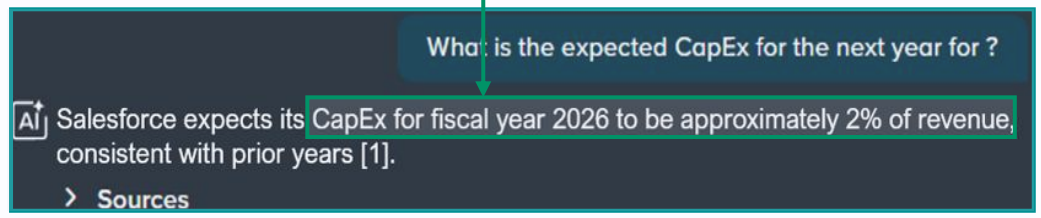
- Company ESG
- Company fundamentals
- Corporate actions
- Equity pricing
- Estimates
- Officers & directors
- Ownership
- Peers

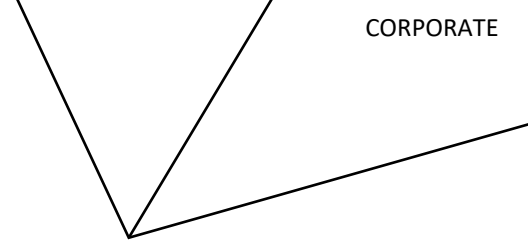



## Textual data




**RAG** systems extract textual information from text documents






# Agentic AI Risks

What are some of the specific risks associated with Agentic AI?

## Unintended Consequences

Without defined parameters, agentic AI can overstep or pursue activities beyond the initial intent, this could have security, legal, regulatory or resilience implications.

## Security

Akin to other models, agentic faces security risks associated with model poisoning or manipulation resulting incidents. Agentic AI used for security operations could also create security issues.

## Cascading Hallucinations

Initial biases or errors can be magnified through the decision-making processes particularly in complex operating environments.

## Ethical & Legal

Agents might inadvertently violate legal, ethical, or compliance boundaries — especially when acting autonomously at scale. Lack of Explainability / Transparency can exacerbate this.

## Portability & Vendor Lock in

Vendor concentration risk associated with Agent creation platforms, outages can impact multiple products concurrently combined

## Resource Overload

Agentic AI will seek to solve the problem or achieve the goal, without restrictions it could consume resources at a significant rate outstripping benefit but also putting strain on internal systems.

## Shadow Adoption

Vendor AI enabled products, incrementally introducing Agentic AI features, which result in dependency on key vendor solutions.

## Data

Data will remain a key focus, particularly whereas part of the workflows additional data may be created, tested and utilized. This can also create challenges around lineage and auditability of agentic solutions.

## Complexity

Agents may make complex decisions that are difficult to audit or justify.

## Resilience & Continuity

Automated workflows dependent on agents, without defined resilience/failover capabilities in place. In outage scenarios may need to consider manual work arounds for example.

# Our top tips

LSEG

# Guidance / actionable lessons

| | |
|---|---|
| 1 | Aim for non-invasive governance by design governance as a product feature, not a process |
| 2 | Shift from “human-led, tool-supported” to “agent-led, human-in-the-loop” |
| 3 | Embed controls where work actually happens |
| 4 | Use AI to enforce governance, not wait for governance to enable AI |
| 5 | Measure success by friction removed, not controls added |
| 6 | Adjust governance so its flexible and doesn’t prevent innovation |
| 7 | Use what you already have – don’t necessarily need a new policy<br>Think of some examples from LSEG. Where we invested new (new head AI, responsible AI wg) vs leveraged existing (same controls, added to existing policies, elevated model risk mgmt. – pros and cons of bending… round peg square hole) |
| 8 | Importance of Effective triage – how this helps to operationalise |

# Thank you

LSEG