DAIG

DATA & AI GOVERNANCE PARTNERS

AI Governance, Responsible AI, and Data Governance

Connecting the Dots

ISACA Belgium Chapter — Online Webinar

Thursday, 21 May 2026 — 17:30 CET

ABOUT

Mathias Vercauteren

International Data & AI Governance Expert

Founder & President · Data & AI Governance Partners

16+ years making data and AI governance work. Not frameworks that sit on shelves — operating capabilities that change how organizations manage data and AI. From a central bank to a global manufacturer, from Washington DC stages to boardrooms across Europe. One practitioner. Global standards. Governance that delivers.

DAMA-DMBOK® 3.0
Global Project Manager

ADGP® Co-Developer
Applied Data Governance Practitioner - Dataversity

Executive PhD
Data Governance · Antwerp Mgmt School

CDMP® Certified
Certified Data Management Professional

11+ International Keynotes
DGIQ · EDW · DMZ · Data & AI Conference

Forthcoming Author
Data Gov Sprint (2026) · AI Gov Sprint (2027)

9 Industries Served over 16+ years
Banking · Healthcare · Gov · Manufacturing +

DAIG
DATA & AI GOVERNANCE
PARTNERS

COMING SOON

The Sprint Series

Two practical playbooks for teams that need governed progress - not endless governance programs.

Data Governance Sprint arrives in late 2026.

AI Governance Sprint follows in 2027.

DATA GOVERNANCE SPRINT
Late 2026

AI GOVERNANCE SPRINT
2027

Author: Mathias Vercauteren | Publisher: Technics Publications

DAIG
DATA & AI GOVERNANCE
PARTNERS

Agenda: where we are headed

1

Assets, Governance & Why It Matters

If governance is asset management, what are we actually managing?

2

AI in 2026

Where we are. Why this matters now.

3

Risks & Failure Modes

What goes wrong when AI is ungoverned.

4

Data Governance

The foundation AI is built on.

5

AI Governance

Definition. Frameworks. Regulation.

6

Responsible AI

The ethical umbrella. Trustworthy AI.

7

Connecting the Dots

One integrated framework.

DAIG
DATA & AI GOVERNANCE
PARTNERS

PART 1

Assets, Governance & Why It Matters

If governance is asset management, what are we actually managing?

DAIG
DATA & AI GOVERNANCE
PARTNERS

Why do

organizations exist?

And what do they need to accomplish their mission?

DAIG
DATA & AI GOVERNANCE
PARTNERS

BlueCross HealthCare

“To be a beacon of excellence in healthcare, providing qualitative, innovative, and patient-centered services that promote wellness and improve the quality of life for the communities we serve.”

Company Objectives:

- Deliver Exceptional Patient Care
- Foster Continuous Improvement
- Expand Community Health

Every company exists to achieve objectives.

To deliver on those objectives, organizations rely on **strategic assets** — the resources, infrastructure, people, capital, technology, and information they need to operate, compete, and **create value**.

These assets aren’t optional. Without them, the organization cannot function. And because they’re critical, they require structured management — oversight, policies, roles, processes, and accountability.

What are STRATEGIC ASSETS?

Strategic assets are the things an organization needs to operate, compete, and create value. They're so critical that without them, the company cannot function. Here are six categories every organization manages:

Equipment & Supplies

The tools of the trade.

For BlueCross Healthcare: MRI machines, surgical instruments, PPE, pharmaceutical inventory.

Locations & Infrastructure

Where work happens.

For BlueCross Healthcare: Hospitals, clinics, offices, warehouses, stations, factories.

Employees & Contractors

The people who deliver.

For BlueCross Healthcare: Doctors, engineers, managers, operators, support staff.

Capital & Expenses & Revenue

The money that flows.

Budgets, investments, operational costs, revenue streams.

Software & Hardware

The technology that enables.

ERP systems, servers, applications, cloud infrastructure.

Data & Analytics Solutions

The intelligence that guides.

Customer data, operational metrics, BI dashboards, reports.

DAIG DATA & AI GOVERNANCE PARTNERS

Assets don’t

manage themselves.

When assets become strategic to an organization,
business functions emerge to manage them.

These functions are the things you do to take care of strategic assets.
They can be considered capabilities.

DAIG
DATA & AI GOVERNANCE
PARTNERS

When assets become strategic, GUARDIANS emerge

Supply Chain	manages →	Equipment & Supplies	✓ Decades of maturity
Facilities Management	manages →	Locations & Infrastructure	✓ Decades of maturity
Human Resources	manages →	Employees & Contractors	✓ Decades of maturity
Finance	manages →	Capital & Revenue	✓ Decades of maturity
Information Technology Governance	manages →	Software & Hardware	✓ Decades of maturity
Data Governance	manages →	**Data & Analytics**	⚠ **Still maturing**

Every company has been down this road of managing assets. Data governance is simply the latest function to develop.

DAIG DATA & AI GOVERNANCE PARTNERS

Not all guardians had the same time to MATURE

Over decades and centuries, some capabilities had time to mature, establish academic foundations, and develop proper oversight. Data governance did not.

Data governance is a theory still being proven. It’s practitioner-led and vendor-driven — without the proper academic foundation that disciplines like finance or HR have had centuries to develop. It’s an unproven theory, and it will need to adapt fast.

Asset management

is boring.

That’s the point.

It’s not new.

Every company has been down this road with other assets. We’re not inventing a new discipline.

It’s not glamorous.

Policies, processes, standards, roles, responsibilities. The plumbing of organizational capability.

It needs to become BAU.

Business as usual. Not a project with an end date. Not a program. A permanent function. An enterprise-wide capability.

DAIG
DATA & AI GOVERNANCE
PARTNERS

The REFRAME: Governance = Asset Management

This is the foundational mental model for everything that follows in this webinar:

HR manages people assets	Finance manages financial assets	Data Gov manages data assets
• Establishes hiring policies • Defines performance standards • Provides tools & systems • Clarifies organizational structure • Enables consistent practices • Addresses employee issues	• Sets financial standards • Defines compliance policies • Provides budgeting tools • Clarifies accountability • Enables consistent practices • Addresses compliance issues	• Defines data standards & policies • Sets quality & compliance rules • Provides templates & expertise • Clarifies data roles & ownership • Enables consistent data mgmt practices • Addresses data quality issues

Data governance does for data what HR does for people and what Finance does for money.
It’s the same structural logic applied to a different asset class.

DAIG DATA & AI GOVERNANCE PARTNERS

Now,

a new asset has arrived.

AI solutions — models, algorithms, chatbots, automated decision systems — are becoming strategic assets. They require the same oversight and control that every other strategic asset demands.

If data needs governance because it's a strategic asset … then AI needs governance for the exact same reason.

DAIG
DATA & AI GOVERNANCE
PARTNERS

Why AI solutions are STRATEGIC ASSETS

AI systems are not just tools — they are becoming core to how organizations operate, decide, and compete:

They make consequential decisions	Credit approvals, medical diagnoses, hiring recommendations, fraud detection — decisions that affect people's lives and livelihoods.
They operate at scale and speed	Processing millions of data points, serving thousands of customers simultaneously, making decisions faster than any human could.
They carry material risk	Bias, errors, security vulnerabilities, regulatory non-compliance, reputational damage — risks that can be existential.
They require ongoing management	Model drift, data quality changes, evolving regulations, new attack vectors — AI systems don't 'set and forget.'
They are becoming competitive differentiators	Organizations that govern AI well can deploy faster, with more confidence, and with greater stakeholder trust.

Any asset that is strategic, consequential, risky, and requires ongoing management needs governance. AI checks every box.

The complete picture: Data & AI Governance

This is the enterprise capability map with AI Governance added as the 7th function. Note how Data Governance and AI Governance sit side by side as the two newest functions — both managing strategic assets that have only recently been recognized as requiring formal governance.

DAIG DATA & AI GOVERNANCE PARTNERS

PART 2

AI in 2026

Where we are. Why this matters now.

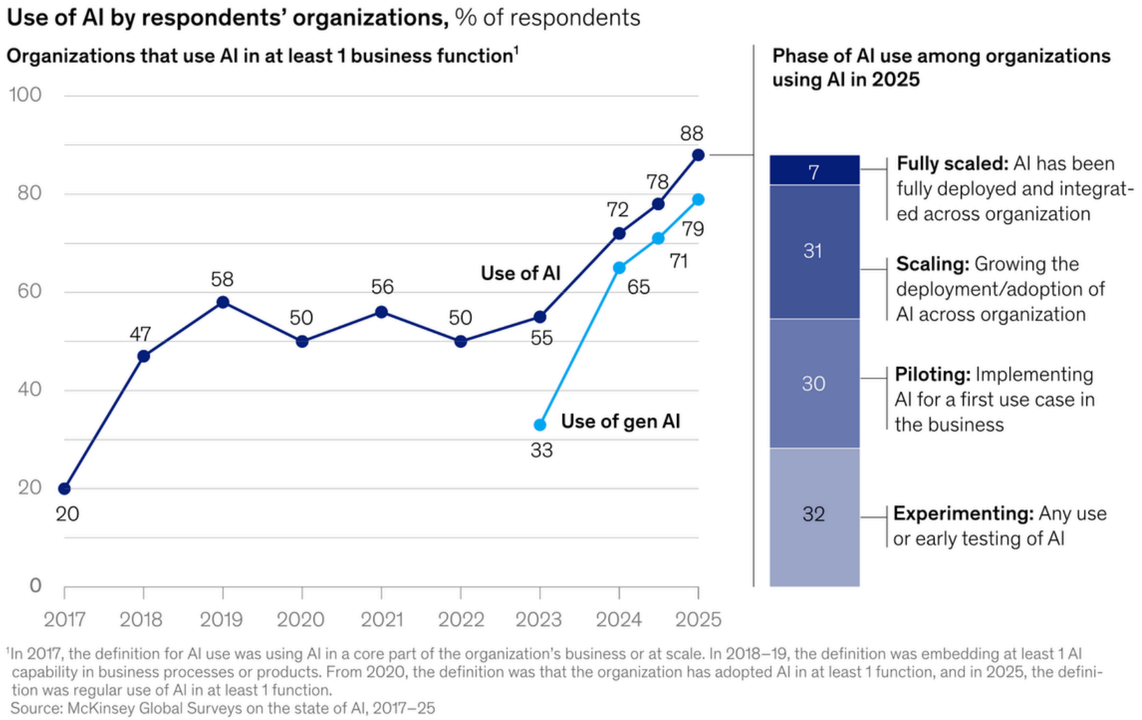
DAIG
DATA & AI GOVERNANCE
PARTNERS

AI moves from experiment to EVERYDAY BUSINESS

More companies than ever now use AI in at least one business function—and the curve is still climbing.

- The share of companies using AI in at least **one business function** continues to rise year over year, signalling that AI has firmly entered mainstream operations.
- Adoption is no longer limited to digital leaders—most industries now report **widespread functional AI use** across marketing, operations, product development, and service.
- Organizations are increasingly moving beyond isolated pilots, **embedding AI into everyday workflows** where the impact is tangible and repeatable.

Reported use of AI in at least one business function continues to increase.



[1]In 2017, the definition for AI use was using AI in a core part of the organization's business or at scale. In 2018–19, the definition was embedding at least 1 AI capability in business processes or products. From 2020, the definition was that the organization has adopted AI in at least 1 function, and in 2025, the definition was regular use of AI in at least 1 function.
Source: McKinsey Global Surveys on the state of AI, 2017–25

Source: McKinsey & Company. (2025, November 5). The state of AI in 2025: Agents, innovation, and transformation. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

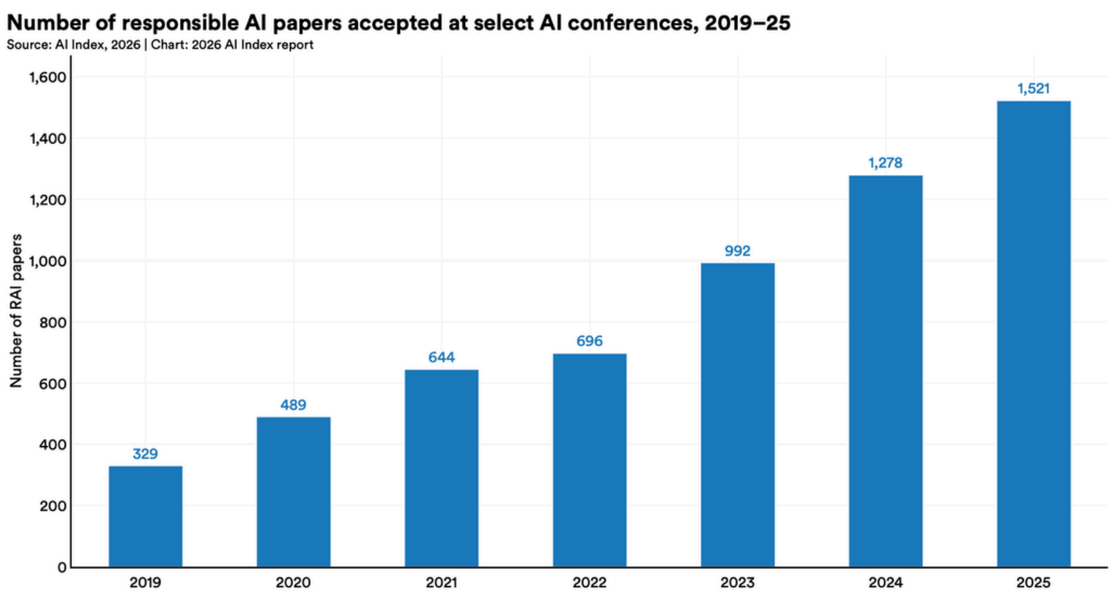
*The competitive gap is shifting from **adoption** to the **effective scaling and governance** of AI systems.*

DAIG DATA & AI GOVERNANCE PARTNERS

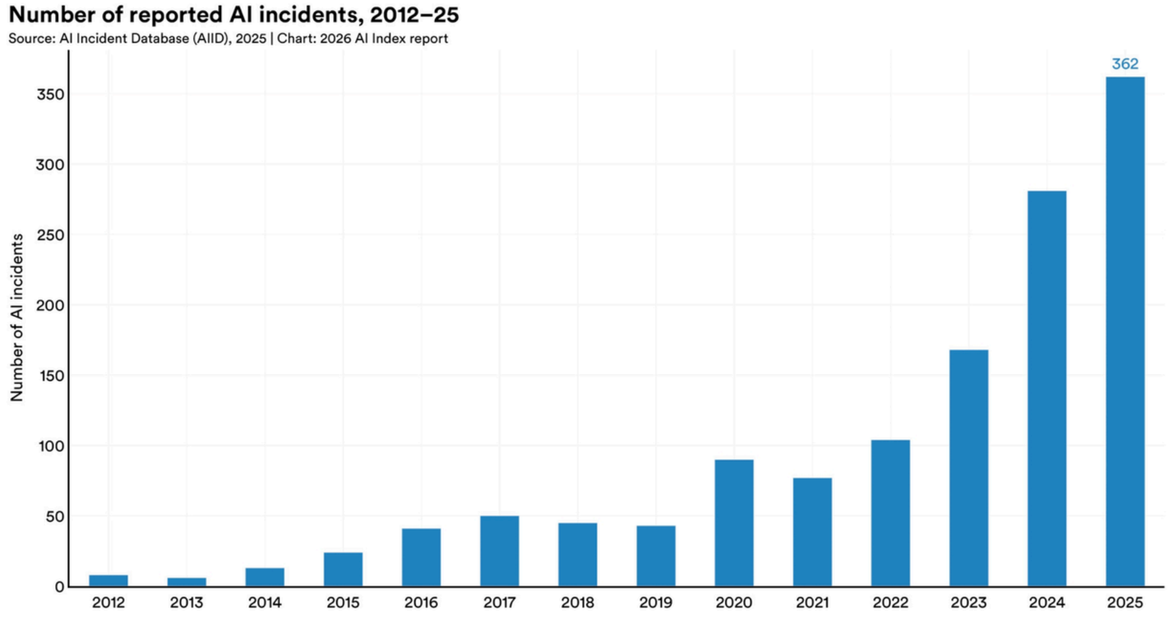
AI Governance is ACCELERATING Globally

Business adoption and regulatory activity surge in 2026.

Organizational adoption rose to **88%** in 2025



The number of responsible AI papers accepted at these conferences has been growing consistently.



Responsible AI is not keeping pace with AI capability, with safety benchmarks lagging and incidents rising sharply.

Source: Stanford University Human-Centered Artificial Intelligence. (2026). The 2026 AI Index report. https://hai.stanford.edu/assets/files/ai_index_report_2026.pdf

DAIG DATA & AI GOVERNANCE PARTNERS

What are we governing? — AI asset's LIFECYCLE

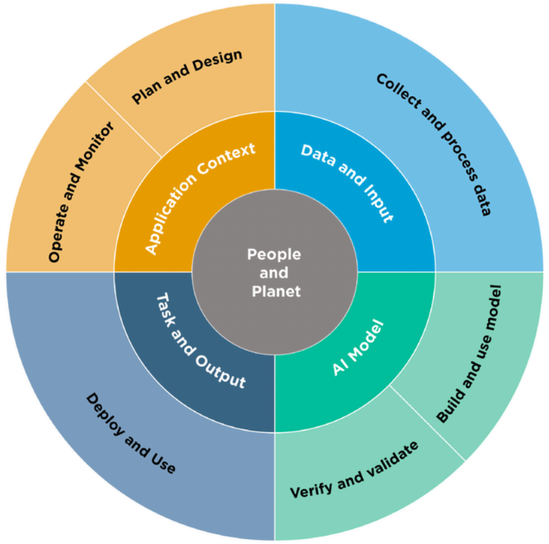


Fig. 2. Lifecycle and Key Dimensions of an AI System. Modified from OECD (2022) OECD Framework for the Classification of AI systems — OECD Digital Economy Papers. The two inner circles show AI systems' key dimensions and the outer circle shows AI lifecycle stages. Ideally, risk management efforts start with the Plan and Design function in the application context and are performed throughout the AI system lifecycle. See Figure 3 for representative AI actors.

Key Dimensions	Application Context	Data & Input	AI Model	AI Model	Task & Output	Application Context	People & Planet
Lifecycle Stage	Plan and Design	Collect and Process Data	Build and Use Model	Verify and Validate	Deploy and Use	Operate and Monitor	Use or Impacted by
TEVV	TEVV includes audit & impact assessment	TEVV includes internal & external validation	TEVV includes model testing	TEVV includes model testing	TEVV includes integration, compliance testing & validation	TEVV includes audit & impact assessment	TEVV includes audit & impact assessment
Activities	Articulate and document the system's concept and objectives, underlying assumptions, and context in light of legal and regulatory requirements and ethical considerations.	Gather, validate, and clean data and document the metadata and characteristics of the dataset, in light of objectives, legal and ethical considerations.	Create or select algorithms; train models.	Verify & validate, calibrate, and interpret model output.	Pilot, check compatibility with legacy systems, verify regulatory compliance, manage organizational change, and evaluate user experience.	Operate the AI system and continuously assess its recommendations and impacts (both intended and unintended) in light of objectives, legal and regulatory requirements, and ethical considerations.	Use system/ technology; monitor & assess impacts; seek mitigation of impacts, advocate for rights.
Representative Actors	System operators; end users; domain experts; AI designers; impact assessors; TEVV experts; product managers; compliance experts; auditors; governance experts; organizational management; C-suite executives; impacted individuals/ communities; evaluators.	Data scientists; data engineers; data providers; domain experts; socio-cultural analysts; human factors experts; TEVV experts.	Modelers; model engineers; data scientists; developers; domain experts; with consultation of socio-cultural analysts familiar with the application context and TEVV experts.		System integrators; developers; systems engineers; software engineers; domain experts; procurement experts; third-party suppliers; C-suite executives; with consultation of human factors experts, socio-cultural analysts, governance experts, TEVV experts,	System operators, end users, and practitioners; domain experts; AI designers; impact assessors; TEVV experts; system funders; product managers; compliance experts; auditors; governance experts; organizational management; impact-ed individuals/commu-nities; evaluators.	End users, operators, and practitioners; impacted individu-als/communities; general public; policy makers; standards organizations; trade associations; advocacy groups; environmental groups; civil society organizations; researchers.

Fig. 3. AI actors across AI lifecycle stages. See Appendix A for detailed descriptions of AI actor tasks, including details about testing, evaluation, verification, and validation tasks. Note that AI actors in the AI Model dimension (Figure 2) are separated as a best practice, with those building and using the models separated from those verifying and validating the models.

Source: National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1). https://doi.org/10.6028/nist.ai.100-1

DAIG DATA & AI GOVERNANCE PARTNERS

PART 3

Risks & Failure Modes

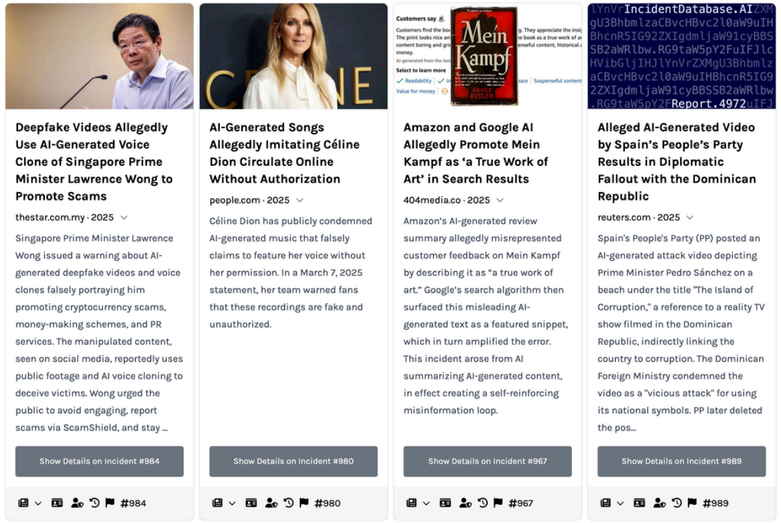
What goes wrong when AI is ungoverned.

DAIG
DATA & AI GOVERNANCE
PARTNERS

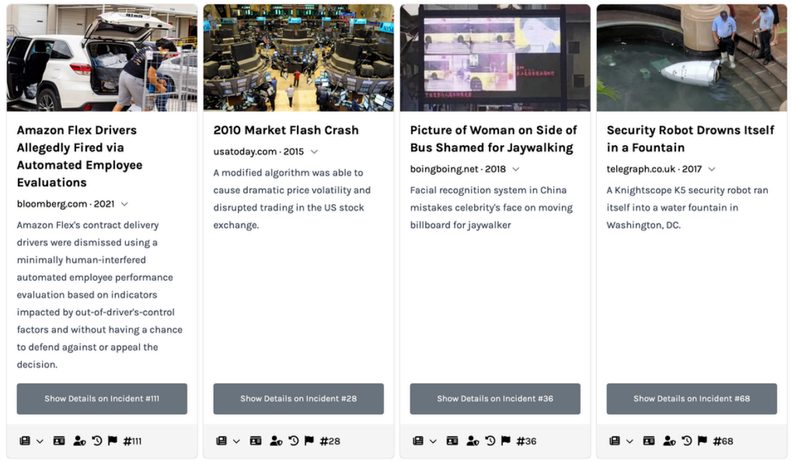
The stakes are BOARD-LEVEL

As AI systems transition from pilot projects to enterprise deployments, risk shifts from theoretical to board-level materiality.

Recent incidents underscore the urgent need for robust AI governance to prevent and manage such occurrences.



Source: The AI Incident Database, Accessed on 15/04/2025. Available at: https://incidentdatabase.ai



Source: WalkMe Team. (2025, June 23). 15 Potential Artificial Intelligence (AI) Risks. https://www.walkme.com/blog/ai-risks/

The AI Incident Database

The AI Incident Database is dedicated to indexing the collective history of harms or near harms realized in the real world by the deployment of artificial intelligence systems.

DAIG DATA & AI GOVERNANCE PARTNERS

Unintended HARM: The core challenge of AI systems

- AI systems, despite their promise, can lead to unintended negative consequences across various domains.
- The NIST AI Risk Management Framework (AI RMF) categorizes these potential harms into three main areas:

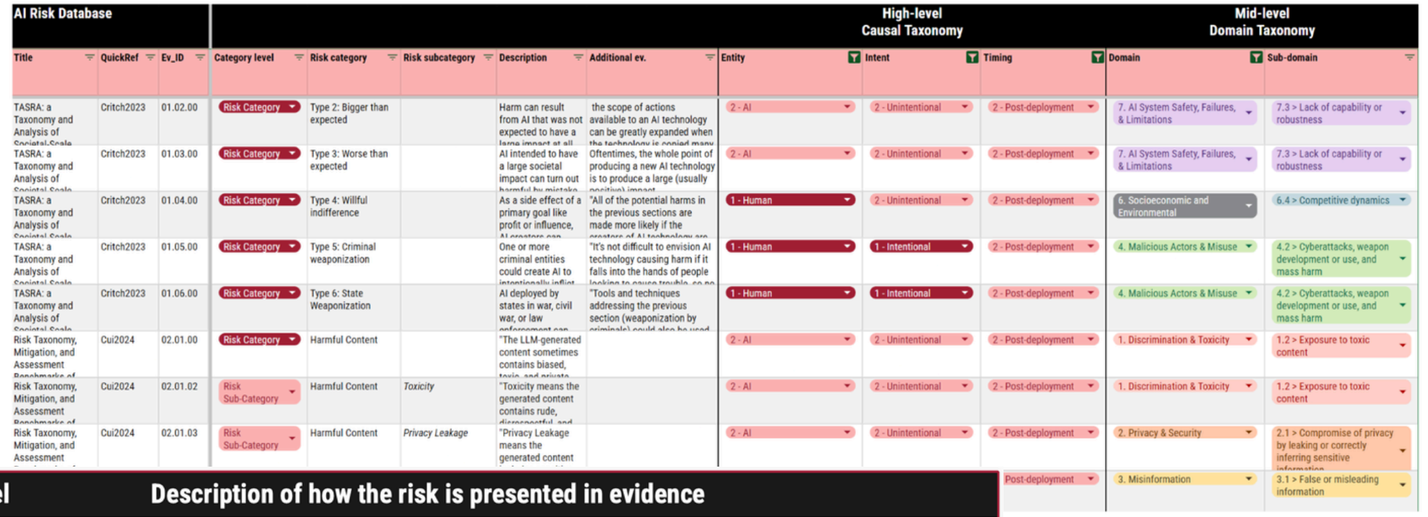
Fig. 1. Examples of potential harms related to AI systems. Trustworthy AI systems and their responsible use can mitigate negative risks and contribute to benefits for people, organizations, and ecosystems.

Source: National Institute of Standards and Technology (NIST) , "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," January 2023. Available at: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

MIT AI RISK Repository

The AI Risk Repository has three parts:

- The **AI Risk Database** captures 1700+ risks extracted from 74 existing frameworks and classifications of AI risks
- The **Causal Taxonomy of AI Risks** classifies how, when, and why these risks occur
- The **Domain Taxonomy of AI Risks** classifies these risks into 7 domains (e.g., “Misinformation”) and 24 subdomains (e.g., “False or misleading information”)



AI Risk Database								High-level Causal Taxonomy			Mid-level Domain Taxonomy	
Title	QuickRef	Ev_ID	Category level	Risk category	Risk subcategory	Description	Additional ev.	Entity	Intent	Timing	Domain	Sub-domain
TASRA: a Taxonomy and Analysis of	Critch2023	01.02.00	Risk Category	Type 2: Bigger than expected		Harm can result from AI that was not expected to have a	the scope of actions available to an AI technology can be greatly expanded when	2 - AI	2 - Unintentional	2 - Post-deployment	7. AI System Safety, Failures, & Limitations	7.3 > Lack of capability or robustness
TASRA: a Taxonomy and Analysis of	Critch2023	01.03.00	Risk Category	Type 3: Worse than expected		AI intended to have a large societal impact can turn out	Oftentimes, the whole point of producing a new AI technology is to produce a large (usually	2 - AI	2 - Unintentional	2 - Post-deployment	7. AI System Safety, Failures, & Limitations	7.3 > Lack of capability or robustness
TASRA: a Taxonomy and Analysis of	Critch2023	01.04.00	Risk Category	Type 4: Willful indifference		As a side effect of a primary goal like profit or influence,	"All of the potential harms in the previous sections are made more likely if the	1 - Human	2 - Unintentional	2 - Post-deployment	6. Socioeconomic and Environmental	6.4 > Competitive dynamics
TASRA: a Taxonomy and Analysis of	Critch2023	01.05.00	Risk Category	Type 5: Criminal weaponization		One or more criminal entities could create AI to	"It's not difficult to envision AI technology causing harm if it falls into the hands of people	1 - Human	1 - Intentional	2 - Post-deployment	4. Malicious Actors & Misuse	4.2 > Cyberattacks, weapon development or use, and mass harm
TASRA: a Taxonomy and Analysis of	Critch2023	01.06.00	Risk Category	Type 6: State Weaponization		AI deployed by states in war, civil war, or law	"Tools and techniques addressing the previous section (weaponization by	1 - Human	1 - Intentional	2 - Post-deployment	4. Malicious Actors & Misuse	4.2 > Cyberattacks, weapon development or use, and mass harm
Risk Taxonomy, Mitigation, and Assessment	Cui2024	02.01.00	Risk Category	Harmful Content		"The LLM-generated content sometimes contains biased,		2 - AI	2 - Unintentional	2 - Post-deployment	1. Discrimination & Toxicity	1.2 > Exposure to toxic content
Risk Taxonomy, Mitigation, and Assessment	Cui2024	02.01.02	Risk Sub-Category	Harmful Content	*Toxicity*	"Toxicity means the generated content contains rude,		2 - AI	2 - Unintentional	2 - Post-deployment	1. Discrimination & Toxicity	1.2 > Exposure to toxic content
Risk Taxonomy, Mitigation, and Assessment	Cui2024	02.01.03	Risk Sub-Category	Harmful Content	*Privacy Leakage*	"Privacy Leakage means the generated content		2 - AI	2 - Unintentional	2 - Post-deployment	2. Privacy & Security	2.1 > Compromise of privacy by leaking or correctly inferring sensitive
										Post-deployment	3. Misinformation	3.1 > False or misleading information

Category	Level	Description of how the risk is presented in evidence
Entity	AI	Due to a decision or action made by an AI system
	Human	Due to a decision or action made by humans
	Other	Due to some other reason or ambiguous
Intent	Intentional	Due to an expected outcome from pursuing a goal
	Unintentional	Due to an unexpected outcome from pursuing a goal
	Other	Without clearly specifying the intentionality
Timing	Pre-deployment	Before the AI is deployed
	Post-deployment	After the AI model has been trained a
	Other	Without a clearly specified time of oc

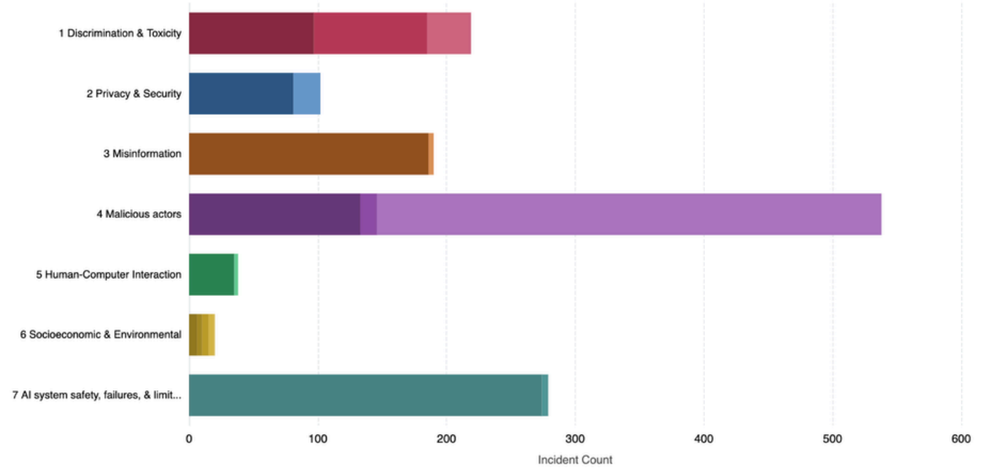
Domain / Subdomain
1 *Discrimination & Toxicity*
1.1 Unfair discrimination and misrepresentation
1.2 Exposure to toxic content
1.3 Unequal performance across groups
2 *Privacy & Security*
2.1 Compromise of privacy by obtaining, leaking or correctly inferring sensitive information
2.2 AI system security vulnerabilities and attacks
3 *Misinformation*
3.1 False or misleading information
3.2 Pollution of information ecosystem and loss of consensus reality
4 *Malicious actors & Misuse*
4.1 Disinformation, surveillance, and influence at scale
4.2 Cyberattacks, weapon development or use, and mass harm
4.3 Fraud, scams, and targeted manipulation

Domain / Subdomain
5 *Human-Computer Interaction*
5.1 Overreliance and unsafe use
5.2 Loss of human agency and autonomy
6 *Socioeconomic & Environmental Harms*
6.1 Power centralization and unfair distribution of benefits
6.2 Increased inequality and decline in employment quality
6.3 Economic and cultural devaluation of human effort
6.4 Competitive dynamics
6.5 Governance failure
6.6 Environmental harm
7 *AI system safety, failures, and limitations*
7.1 AI pursuing its own goals in conflict with human goals or values
7.2 AI possessing dangerous capabilities
7.3 Lack of capability or robustness
7.4 Lack of transparency or interpretability
7.5 AI welfare and rights
7.6 Multi-agent risks

Source: MIT AI Risk Repository, Accessed 15/04/2025. Available at: https://airisk.mit.edu

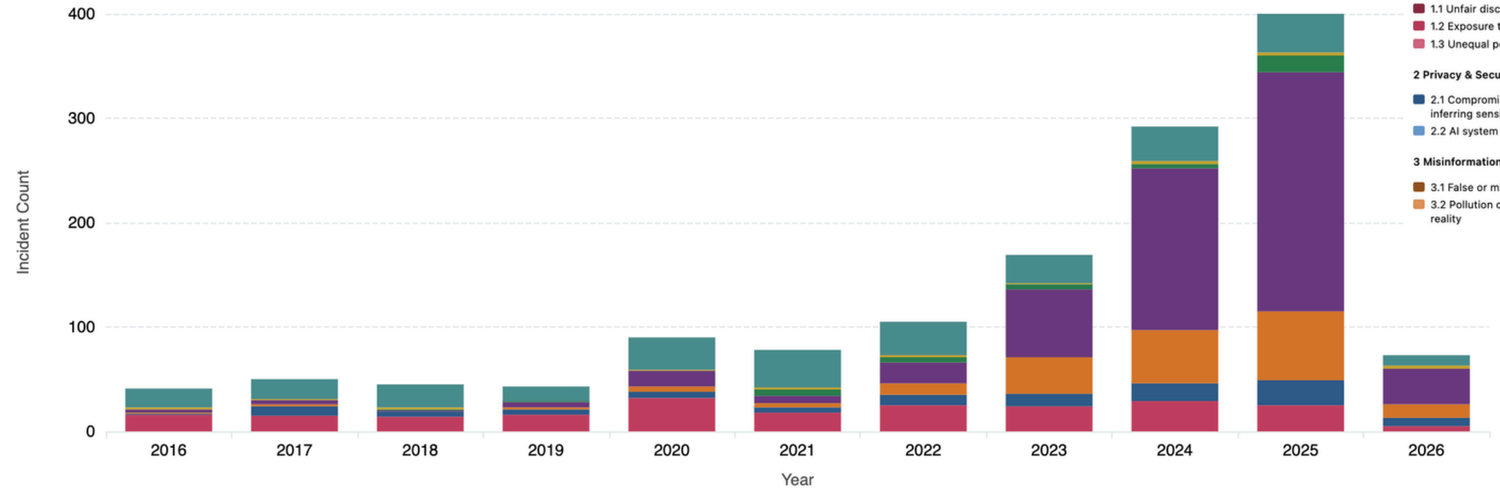
DAIG DATA & AI GOVERNANCE PARTNERS

MIT AI Risk Repository - Risk CLASSIFICATION



How are numbers of reported AI Incidents changing over time?

Stack by Domain + Add filter Severity



Risk Subdomains: *(click categories to toggle visibility)*

1 Discrimination & Toxicity
- 1.1 Unfair discrimination and misrepresentation
- 1.2 Exposure to toxic content
- 1.3 Unequal performance across groups

2 Privacy & Security
- 2.1 Compromise of privacy by obtaining, leaking or correctly inferring sensitive information
- 2.2 AI system security vulnerabilities and attacks

3 Misinformation
- 3.1 False or misleading information
- 3.2 Pollution of information ecosystem and loss of consensus reality

4 Malicious actors
- 4.1 Disinformation, surveillance, and influence at scale
- 4.2 Cyberattacks, weapon development or use, and mass harm
- 4.3 Fraud, scams, and targeted manipulation

5 Human-Computer Interaction
- 5.1 Overreliance and unsafe use
- 5.2 Loss of human agency and autonomy

6 Socioeconomic & Environmental
- 6.1 Power centralization and unfair distribution of benefits
- 6.2 Increased inequality and decline in employment quality
- 6.3 Economic and cultural devaluation of human effort
- 6.4 Competitive dynamics
- 6.5 Governance failure
- 6.6 Environmental harm

7 AI system safety, failures, & limitations
- 7.1 AI pursuing its own goals in conflict with human goals or values
- 7.3 Lack of capability or robustness
- 7.4 Lack of transparency or interpretability

View by: Proportion of reported incidents

Domains: *(click categories to toggle visibility)*

1 Discrimination & Toxicity | 2 Privacy & Security | 3 Misinformation | 4 Malicious actors | 5 Human-Computer Interaction | 6 Socioeconomic & Environmental | 7 AI system safety, failures, & limitations

Source: MIT AI Risk Repository, Accessed 21/05/2026. Available at: https://airisk.mit.edu

DAIG DATA & AI GOVERNANCE PARTNERS

PART 4

Data Governance

The foundation AI is built on.

DAIG
DATA & AI GOVERNANCE
PARTNERS

AI is fueled

by data.

AI systems learn patterns, make predictions, and generate content based on the information they are trained on. The quality, quantity, and relevance of the data directly determine the capabilities and limitations of any AI application.

Without sufficient and appropriate data, even the most sophisticated AI algorithms will produce unreliable or biased outcomes.

DAIG
DATA & AI GOVERNANCE
PARTNERS

The quality equation: Data in → AI out

The quality of AI outputs is directly determined by the quality of data inputs.

This is an operational reality with measurable consequences:

Credit Scoring	Model trained on biased historical lending data → **Produces discriminatory outcomes that deny loans to qualified applicants from protected groups**
Medical Diagnostics	AI trained on incomplete patient records → **Misses critical conditions in underrepresented populations, leading to delayed treatment**
Fraud Detection	Built on poorly documented data without lineage → **Generates excessive false positives that erode customer trust and waste investigation resources**
Hiring Algorithm	Trained on historical hiring data reflecting past biases → **Systematically filters out qualified candidates from certain demographics**

Every one of these failures traces back to a data governance failure: quality, documentation, lineage, or access control.

DAIG DATA & AI GOVERNANCE PARTNERS

Data is a strategic asset

AI didn't make data valuable. AI made the consequences of ungoverned data unavoidable.

Why data is strategic

Consequential

It drives decisions about people, money, products, and operations.

Risky

Bias, breach, misuse, drift — all carry legal, ethical and operational consequence.

Scalable

Decisions made on data multiply at machine speed when AI is involved.

Long-lived

Once embedded in models and reports, bad data echoes for years.

What does AI specifically need from data?

Quality

Accurate, complete, consistent, timely.
Poor quality = poor learning + poor predictions.

Quantity

Many AI techniques (especially deep learning) need volume.
Too little = overfit, brittle generalization.

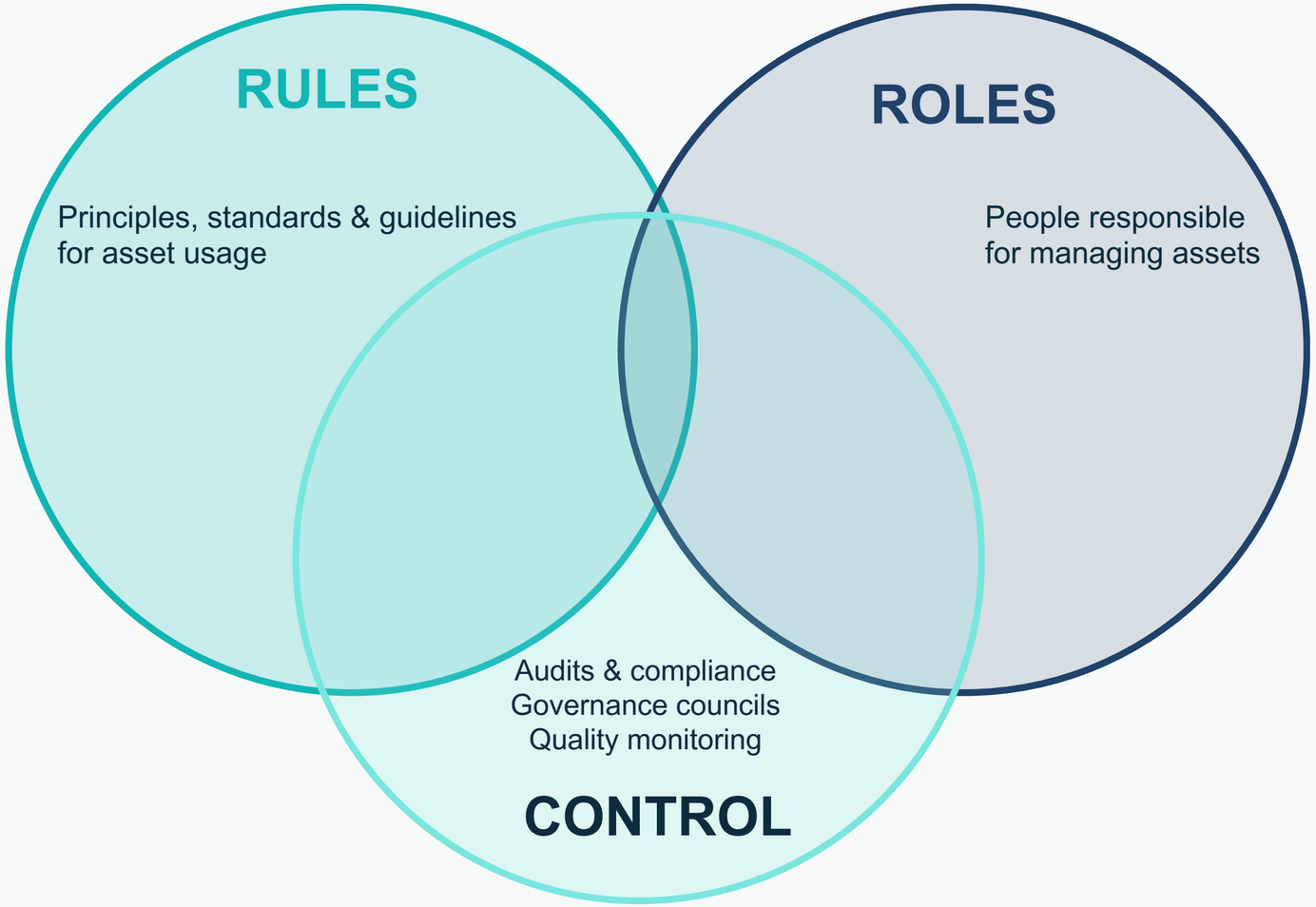
Relevance

Features must actually relate to what the AI is asked to predict.
Otherwise: noise dressed as signal.

Without governed data, AI inherits every silent dysfunction your data already has — and amplifies it.

DAIG
DATA & AI GOVERNANCE
PARTNERS

Rules. Roles. Control.



This is the architecture that applies to every strategic asset.

For data.
For AI.
For anything your organization decides is worth governing.

What is DATA GOVERNANCE?

The exercise of authority, control, and shared decision-making (planning, monitoring, and enforcement) over the management of data assets. — DAMA-DMBOK®

Data governance operates through three interdependent mechanisms:

RULES

The standards and guidelines for data use

Purpose: Define how data should be managed to maintain quality, ensure compliance, and protect sensitive information.

Examples:
- Data privacy policies
- Data quality standards
- Access control protocols
- Retention and archival rules

ROLES

The people responsible for managing data

Purpose: Establish accountability, define responsibilities, and ensure collaboration across the organization.

Examples:
- Data Stewards
- Data Owners
- Data Custodians
- Data Governance Council

CONTROL

The mechanisms ensuring compliance

Purpose: Monitor adherence to rules, enforce policies, and mitigate risks through oversight and governance structures.

Examples:
- Data audits and compliance reviews
- Governance councils or committees
- Data quality monitoring dashboards
- Escalation and remediation processes

Rules, Roles, and Control work together to turn data into a valuable, trusted asset.

DAIG DATA & AI GOVERNANCE PARTNERS

PART 5

AI Governance

Definition. Frameworks. Regulation.

DAIG
DATA & AI GOVERNANCE
PARTNERS

What is AI GOVERNANCE?

Effective AI governance is a comprehensive framework that bridges and combines strategies, policies and processes, connecting business ambition, ethical intent and operational execution into a coherent system, ensuring AI can be trusted and scaled responsibly. — World Economic Forum

Source: World Economic Forum, "Why effective AI governance is becoming a growth strategy, not a constraint," Andrew Wells, 16 Jan. 2026. Available at: https://www.weforum.org/stories/2026/01/why-effective-ai-governance-is-becoming-a-growth-strategy/

AI governance operates through the same three mechanisms:

RULES

The standards and guidelines for AI use

Purpose: Define how AI should be developed, deployed, and managed to ensure safety, fairness, and compliance.

Examples:
- AI ethics principles
- Acceptable use policies
- Risk appetite statements
- Third-party AI vendor policies
- Decommissioning criteria

ROLES

The people responsible for managing AI

Purpose: Establish accountability, define responsibilities, and ensure collaboration across the AI lifecycle.

Examples:
- AI Product Owner
- Model Risk Manager
- AI Operations (MLOps)
- Validation / Challenge Function
- AI Governance Council

CONTROL

The mechanisms ensuring compliance

Purpose: Monitor adherence to rules, enforce policies, and mitigate AI risks through oversight and governance structures.

Examples:
- Bias testing and fairness audits
- Model performance monitoring
- Human oversight mechanisms
- Change control and versioning
- Audit trails and documentation

Rules, Roles, and Control work together to turn AI into a trustworthy, governed asset — the same DNA as data governance.

DAIG DATA & AI GOVERNANCE PARTNERS

Same DNA, different expression

Data governance and AI governance share the same architectural foundation but differ in what they govern:

Dimension	Data Governance	AI Governance
What it governs	Data quality, lineage, access, documentation, stewardship	Model performance, fairness, robustness, lifecycle integrity
Primary asset	Data & analytics solutions	AI models, algorithms, automated decision systems
Core mechanisms	Rules, Roles, Control	Rules, Roles, Control
Key roles	Data Steward, Data Owner, Data Custodian	AI Product Owner, Model Risk Manager, AI Ops
Key processes	Quality monitoring, metadata mgmt, access control	Risk classification, TEVV, deployment gates, PMM
Key artifacts	Business glossary, data dictionary, quality dashboard	Model cards, risk register, technical files
Primary regulations	GDPR, sector-specific data laws	EU AI Act, NIST AI RMF, ISO/IEC 42001

The architecture is identical. The content differs.

The DEPENDENCY CHAIN: AI Governance needs Data Governance

AI governance cannot function without mature data governance. Every AI governance artifact depends on a data governance input:

AI Risk Classification	→ *depends on*	Data lineage and provenance
Model Training & Validation	→ *requires*	Data quality and completeness
Fairness & Bias Assessment	→ *requires*	Demographic data documentation
Model Cards & Datasheets	→ *built from*	Metadata and data dictionaries
Post-Market Monitoring	→ *extends*	Data quality monitoring
Regulatory Compliance (EU AI Act)	→ *layered on*	GDPR compliance and DPIAs

Without data governance, AI governance is building on sand.

DAIG DATA & AI GOVERNANCE PARTNERS

INTEGRATION is possible but with different concerns.

Integration is structurally possible because the foundations are shared — and it is necessary because AI introduces concerns data governance never had to manage.

WHERE THEY OVERLAP — INTEGRATE, DON'T DUPLICATE

1. **Roles & Decision Rights**
   Data Steward role extends to AI data lineage, licensing, and consent. No new role hierarchy needed.
2. **Operating Models**
   Single governance council with AI-specific sub-groups — not two parallel structures.
3. **Policy Frameworks**
   Same hierarchy (principles → policies → standards → procedures). Different content.
4. **Measurement & Monitoring**
   Combined scorecards with data quality and AI fairness/drift in one executive view.
5. **Communication & Training**
   Joint data fluency and AI literacy programs, one Business Glossary, one change story.

WHERE AI GOV ADDS NEW CONCERNS

1. **Risk Classification**
   By level of automation and impact on fundamental rights. Data Gov classifies sensitivity — not autonomy.
2. **Lifecycle Controls**
   Pre-design, TEVV, deployment gates, post-market monitoring, decommissioning — full AI lifecycle.
3. **AI-Specific Regulation**
   EU AI Act conformity assessment, Technical File, NIST AI RMF, ISO/IEC 42001. Distinct from GDPR.
4. **Third-Party AI Risk**
   Foundation models, API services, embedded AI in SaaS. Model transparency, testing rights, liability.

The architecture is identical. The content differs. Integrate, don't duplicate.

DAIG DATA & AI GOVERNANCE PARTNERS

AI GOVERNANCE is in its early stages

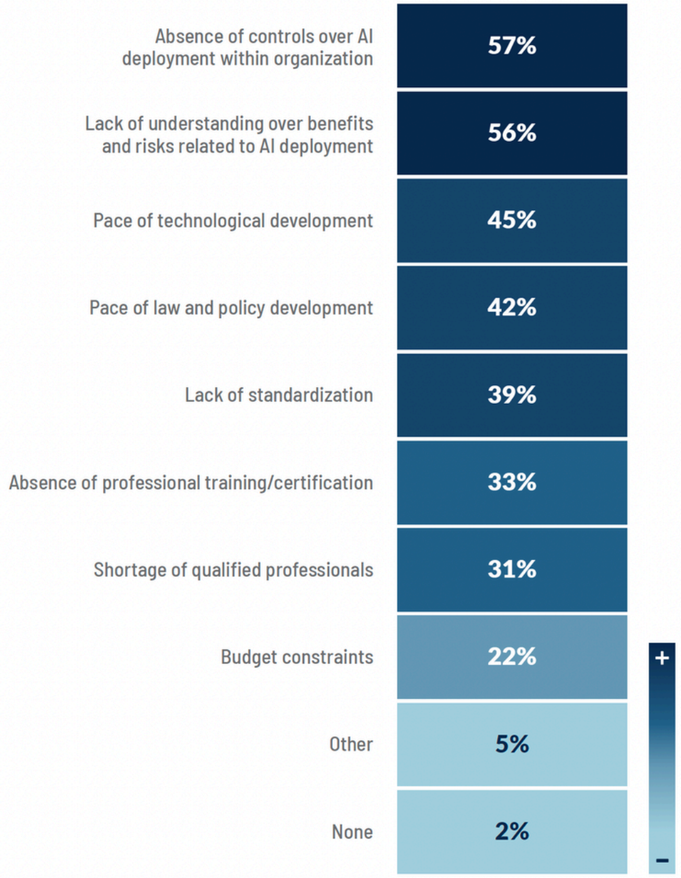
Challenges and slow-ish implementation are still common and there's no standard governance framework (yet).

IAPP's definition

Organizational AI governance refers to the internal guidelines and practices organizations follow to ensure responsible development, deployment or use of AI by that organization.

iapp | EY

Most common AI governance challenges faced by organizations



Existence of an AI governance function by annual revenue in USD

	Overall	Under 100 million	100-999 million	1-8.9 billion	9-19.9 billion	20-59.9 billion	More than 60 billion
Established AI governance function	29%	17%	26%	31%	18%	38%	52% ↑
Likely to establish an AI governance function in the next 12 months	31%	28%	31%	31%	39%	29%	26%
No established AI governance function	35%	45%	39%	34%	34%	32%	13% ↓
Unsure	6%	11%	4%	5%	8%	0%	10%

Existence of an AI governance function by number of employees

	Overall	Under 100	100-999	1,000-4,999	5,000-24,999	25,000-79,999	More than 80,000
Established AI governance function	29%	21%	18%	22%	34%	27%	45% ↑
Likely to establish an AI governance function in the next 12 months	31%	21%	29%	27%	37%	27%	30%
No established AI governance function	35%	43%	49% ↑	46% ↑	27% ↓	30%	20% ↓
Unsure	6%	14%	4%	5%	3%	16% ↑	5%

Existence of an AI governance function by respondent's confidence in privacy compliance

	Overall	Not at all confident	Somewhat confident	Totally confident
Established AI governance function	29%	12% ↓	30%	32%
Likely to establish an AI governance function in the next 12 months	31%	19%	31%	37%
No established AI governance function	35%	65% ↑	33%	28%
Unsure	6%	4%	7%	4%

Source: International Association of Privacy Professionals & EY. (2023). IAPP–EY professionalizing organizational AI governance report. IAPP. https://iapp.org/media/pdf/resource_center/iapp_ey_professionalizing_organizational_ai_governance_report.pdf

DAIG DATA & AI GOVERNANCE PARTNERS

Global AI Law and Policy TRACKER

This tracker identifies AI legislative and policy developments in a subset of jurisdictions.

Jurisdictions in focus

Argentina
Australia
Bangladesh
Brazil
Canada
Chile
China
Colombia
Egypt
EU
India
Indonesia
Israel
Japan
Mauritius
New Zealand
Nigeria
Peru
Saudi Arabia
Singapore
South Korea
Taiwan
United Arab Emirates
U.K.
U.S.

Region	Sovereignty	Assets
N. America	USA	Algorithmic Accountability Act (draft), NIST AI Risk Management Framework, E.O. 13960, E.O. 14110, Blueprint for an AI Bill of Rights, AI Safety Institute
	Canada	AI & Data Act (proposed), GenAI Code of Practice,
APAC	Australia	AI Ethics Framework, AI Ethics Principles, AI Standards Roadmap
	China	AI Guidelines, Summary of regulations
	India	Digital India Act, 2023 (proposed), India AI program
	Japan	Social Principles of Human-Centric AI
	New Zealand	Algorithm Charter, Trustworthy AI in Aotearoa principles
	Singapore	Model AI Governance Framework, VerifyAI, Model AI Governance Framework for Generative AI
LATAM	Argentina	Provision 2/2023 (published), Law 27,699, Resolution 161/23
	Brazil	Bill No. 2338/2023 (proposed)
	Chile	National Policy and Action Plan on AI
EMEA	EU	EU AI Act (approved)
	UK	AI Standards, AI Standards Hub
Global Agreements & Standards	Bletchley	Bletchley Declaration (AI Safety)
	G7	Hiroshima AI Process, AI Code of Conduct
	OECD	AI Principles
	UNESCO	AI Ethics

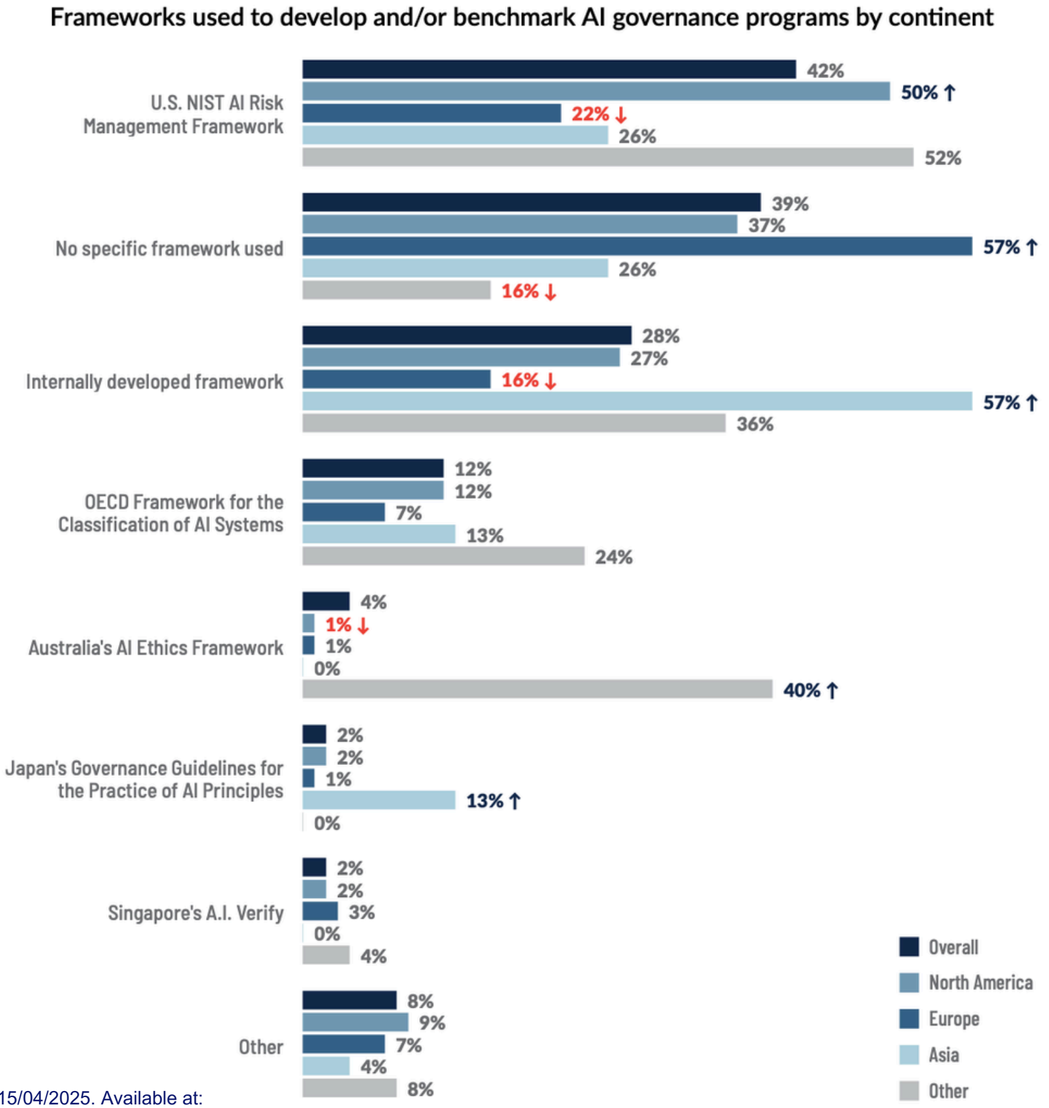
Source: International Association of Privacy Professionals (IAPP), "Global AI Law and Policy Tracker," Accessed on 15/04/2025. Available at: https://iapp.org/resources/article/global-ai-legislation-tracker/

DAIG DATA & AI GOVERNANCE PARTNERS

Use of AI Governance FRAMEWORKS

- Organizations primarily use **governmental frameworks**, notably the U.S. NIST AI Risk Management Framework (42%) and internally developed frameworks (28%); there's a notable overlap where 60% using NIST AI RMF also employ the NIST Privacy Framework, reflecting privacy governance's maturity.

- **Regional Differences:** Framework choice strongly correlates with geography—NIST AI RMF usage is high in North America, Japan's AI governance guidelines dominate in Asia, and Europe notably lacks a specific AI governance framework (57% use none), likely awaiting the EU AI Act for regulatory clarity.

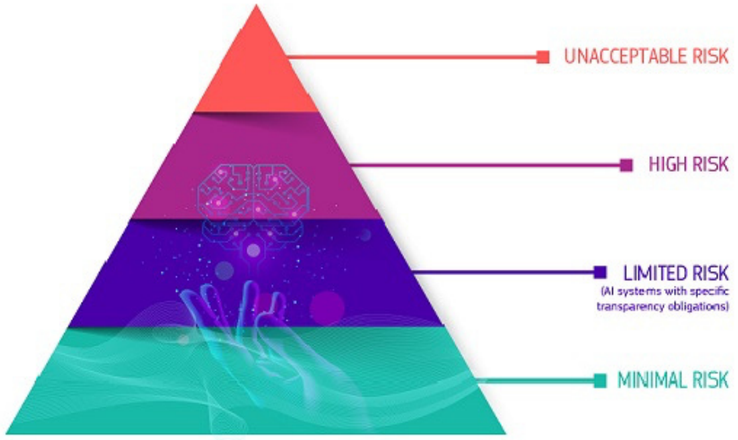


Source: International Association of Privacy Professionals (IAPP) & EY, "IAPP-EY Professionalizing Organizational AI Governance Report," Accessed on 15/04/2025. Available at: https://iapp.org/media/pdf/resource_center/iapp_ey_professionalizing_organizational_ai_governance_report.pdf

DAIG DATA & AI GOVERNANCE PARTNERS

AI Governance frameworks and REGULATIONS

In the rapidly evolving AI landscape, businesses face new rules and standards to ensure trustworthy and responsible AI. Organizations must navigate both government regulations and voluntary frameworks to manage AI risks and compliance.



EU AI Act

Source: *EU AI Act - Official Portal*

NIST Risk Management Framework

Source: *NIST AI Risk Management Framework*

ISO/IEC 42001

Source: *ISO/IEC 42001 – AI Management System Standard*

DAIG DATA & AI GOVERNANCE PARTNERS

EU AI Act: delay compliance date for high-risk AI systems to 2 December 2027

European Commission

EN

Shaping Europe's digital future

Home | Policies | Activities | News | Library | Funding | Calendar | Consultations | AI Office

Home > News & Views > EU agrees to simplify AI rules to boost innovation and ban 'nudification' apps to protect citizens

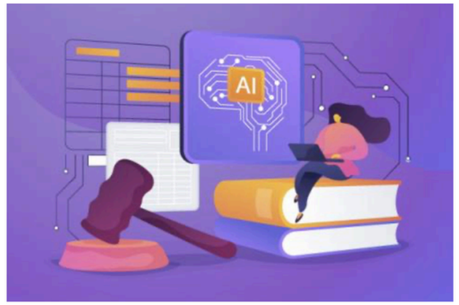
EU agrees to simplify AI rules to boost innovation and ban 'nudification' apps to protect citizens

PRESS RELEASE
Publication 07 May 2026

The European Commission welcomes the political agreement reached between the European Parliament and the Council of the EU on simpler, innovation-friendly rules for artificial intelligence (AI).

The Commission proposed the Digital Omnibus on AI only five months ago as part of the EU's simplification agenda to boost Europe's competitiveness. This will make the implementation of the AI Act for EU businesses easier while maintaining its benefits for European society, safety and fundamental rights.

Today's agreement sets a clear implementation timeline for the rules governing high-risk AI systems. Rules for systems used in certain high-risk areas — including biometrics, critical infrastructure, education, employment, migration, asylum and border control — will apply from 2 December 2027. For systems integrated into products such as lifts or toys, the rules will apply from 2 August 2028. This sequencing will help ensure that technical standards and other support tools are in place before the rules start to apply.



Related topics

Artificial intelligence | An agile rulebook

Source: European Commission. (2026, May 7). EU agrees to simplify AI rules to boost innovation and ban 'nudification' apps to protect citizens. Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/news/eu-agrees-simplify-ai-rules-boost-innovation-and-ban-nudification-apps-protect-citizens

DAIG DATA & AI GOVERNANCE PARTNERS

PART 6

Responsible AI

The ethical umbrella — and how it differs from AI Governance.

DAIG
DATA & AI GOVERNANCE
PARTNERS

What is RESPONSIBLE AI?

Definition (Virginia Dignum)

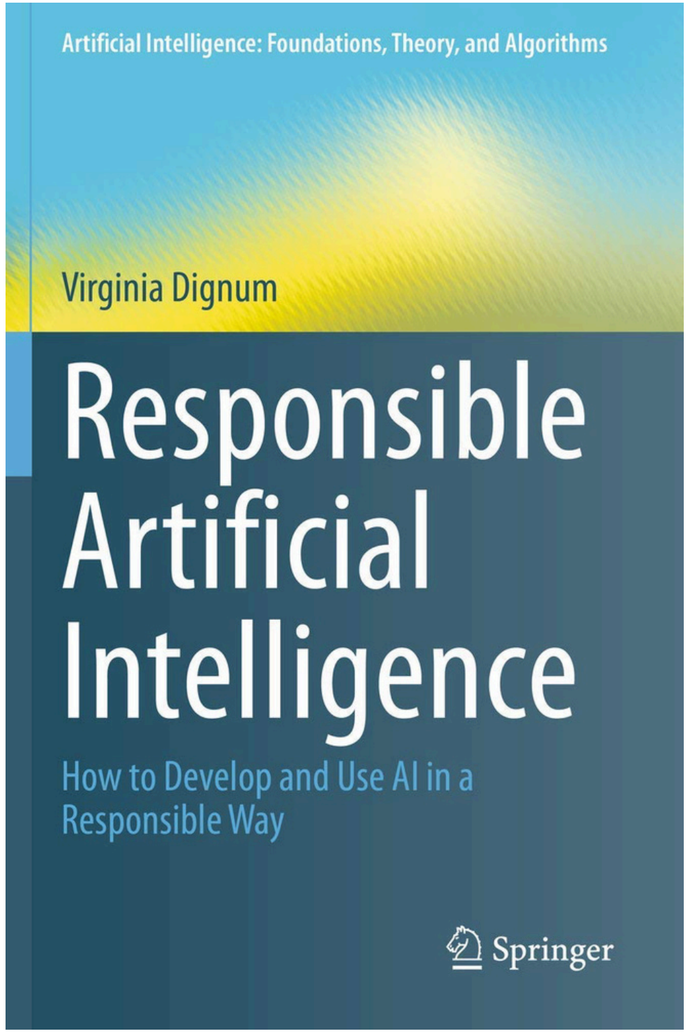
"Responsible AI is about **human responsibility** for the development of intelligent systems along fundamental human principles and values, to ensure human-flourishing and well-being in a sustainable world. … **Responsible AI is not about the characteristics of AI systems**, but about our own role. We are responsible for how we build systems, how we use systems and how much we enable these systems to decide and act by themselves."

Source: Virginia Dignum, Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way, Springer International Publishing, 2019. Available at: https://link.springer.com/book/10.1007/978-3-030-30371-6

Definition (SiliconANGLE)

"Responsible AI is an **umbrella term** for aspects of making appropriate business and ethical choices when adopting AI. It encompasses **decisions around business and societal value, risk, trust, transparency, fairness, bias, mitigation, explainability, accountability, safety, privacy, regulatory compliance and more**. Before organizations design their AI strategy, they must define what responsible AI means within the context of their organization's environment."

Source: SiliconANGLE, "How IT leaders can embrace responsible AI," September 11, 2022. Available at: https://siliconangle.com/2022/09/11/leaders-can-embrace-responsible-ai/



DAIG DATA & AI GOVERNANCE PARTNERS

Global AI Ethics FRAMEWORKS

Three Pillars of Global AI Ethics Standards

OECD AI Principles

1. Inclusive growth, sustainable development, and well-being
2. Human rights and democratic value, incl. fairness and privacy
3. Transparency and explainability
4. Robustness, security, and safety
5. Accountability

Adopted by 47 countries, these principles shape national AI strategies and create a foundation for cross-jurisdictional compliance.

Source: Organisation for Economic Co-operation and Development (OECD), "OECD AI Principles," Adopted May 2019 (updated 2024). Available at: https://www.oecd.org/en/topics/sub-issues/ai-principles.html

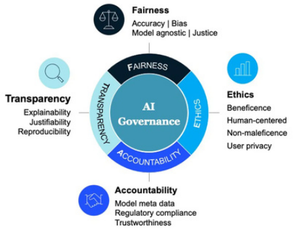
EU HLEG Requirements

1. Human agency and oversight
2. Technical robustness and safety
3. Privacy and data governance
4. Transparency
5. Diversity, non-discrimination, and fairness
6. Societal and environmental well-being
7. Accountability

Over 500 stakeholders contributed. Provides detailed assessment criteria for system-level evaluation.

Source: European Commission, High-Level Expert Group on Artificial Intelligence (AI HLEG), "Ethics Guidelines for Trustworthy AI," 8 April 2019. Available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

FEAT Principles



1. Fairness
2. Ethics
3. Accountability
4. Transparency

The FEAT framework helps guide the development and deployment of AI systems to ensure they are ethical, responsible, and trustworthy.

Source: Monetary Authority of Singapore (MAS), "Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector," 2018 (updated). Available at: https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf

Image Source FEAT: https://medium.com/digital-mckinsey/using-the-feat-approach-to-avoid-biased-ai-f86471bf9d5b

Key Takeaway

These frameworks converge on similar themes, creating a common global language for **responsible AI and AI ethics** that facilitates international cooperation and regulatory alignment. Organizations implementing AI governance should map their controls to multiple frameworks to demonstrate comprehensive compliance and build stakeholder trust across jurisdictions.

DAIG DATA & AI GOVERNANCE PARTNERS

Characteristics of TRUSTWORTHY AI Systems

Characteristics of trustworthy AI systems include: **valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with harmful bias managed.** Creating trustworthy AI requires balancing each of these characteristics based on the AI system's context of use.

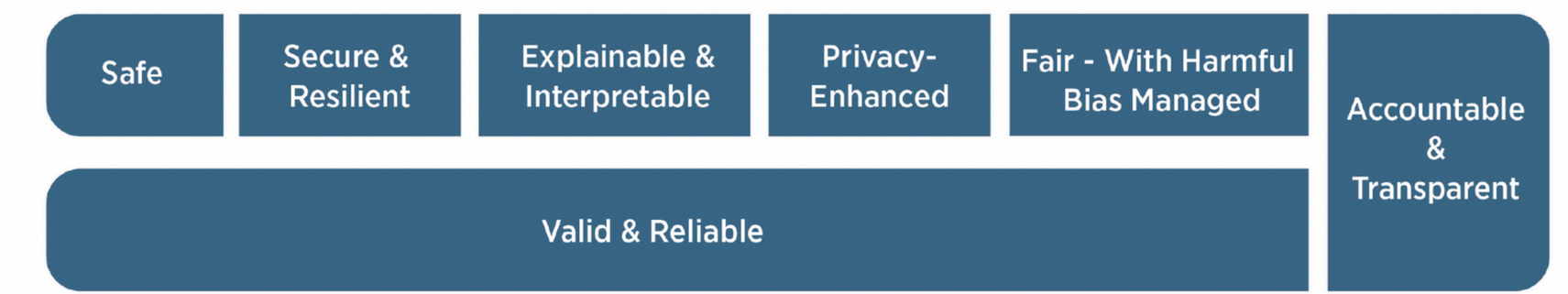


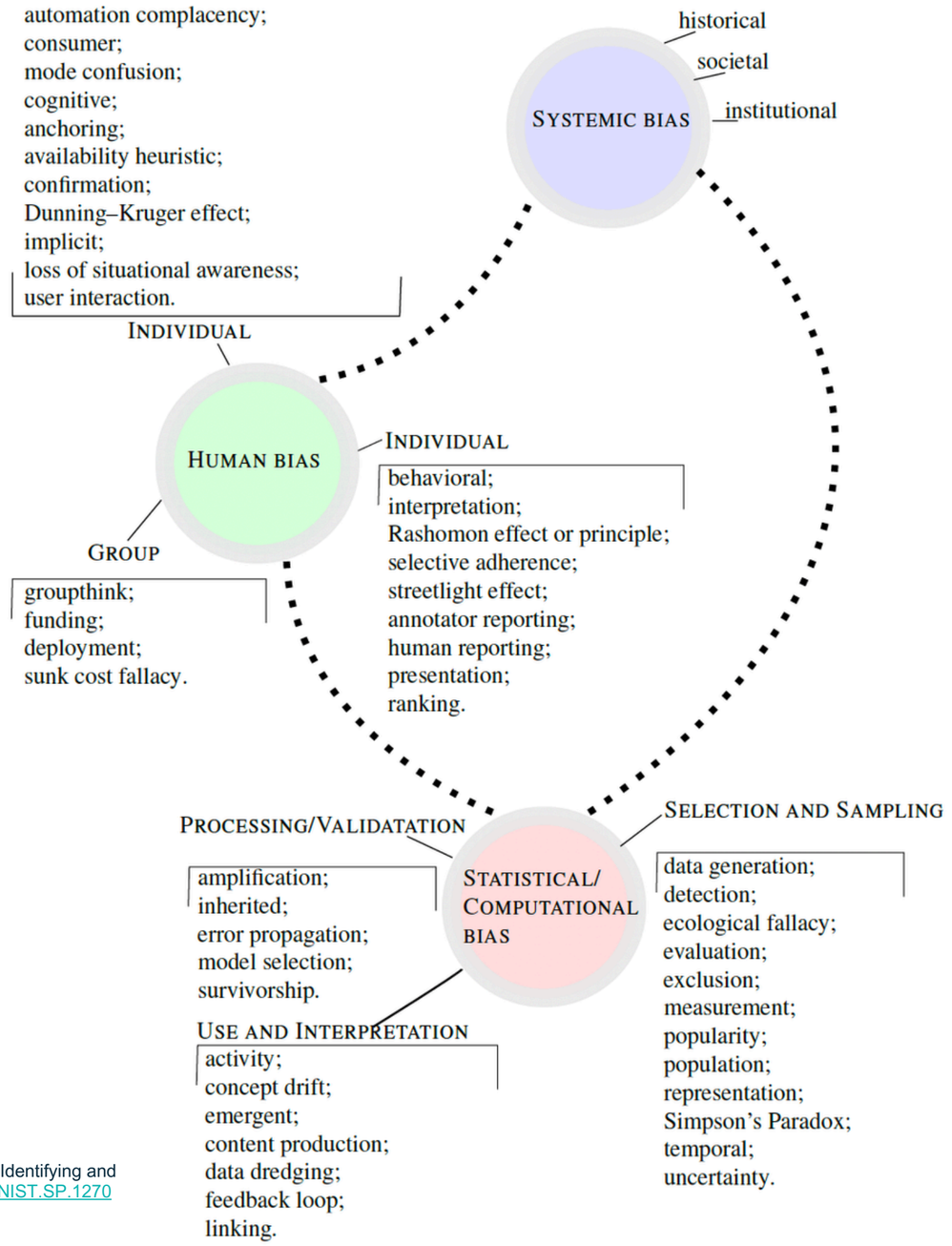
Fig. 4. Characteristics of trustworthy AI systems. Valid & Reliable is a necessary condition of trustworthiness and is shown as the base for other trustworthiness characteristics. Accountable & Transparent is shown as a vertical box because it relates to all other characteristics.

Source: National Institute of Standards and Technology (NIST) , "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," January 2023. Available at: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

DAIG DATA & AI GOVERNANCE PARTNERS

The NIST Socio-Technical LENS: Unpacking the layers of AI bias

- NIST identifies three major categories of AI bias:
  - **Systemic Bias:** Present in AI datasets, organisational norms, practices, processes across the AI lifecycle, and the broader society that uses AI systems.
  - **Human-Cognitive Biases:** Relate to how individuals or groups perceive AI system information, make decisions, or fill in missing information, often influenced by their existing beliefs and heuristics.
  - **Statistical and Computational Biases:** Stem from systematic errors in AI datasets and algorithmic processes, often due to non-representative samples.
- The socio-technical approach highlights that mitigating AI bias requires interdisciplinary collaboration and a holistic understanding of the AI ecosystem.



Source: National Institute of Standards and Technology (NIST), "Towards a Standard for Identifying and Managing Bias in Artificial Intelligence," March 2022. Available at: https://doi.org/10.6028/NIST.SP.1270

DAIG DATA & AI GOVERNANCE PARTNERS

How biases contribute to HARMS

Fig. 5 provides examples of how the three categories of bias—systemic, statistical and computational, and human - interact and contribute to harms within the data and processes used in AI applications, and the validation procedures for determining performance.

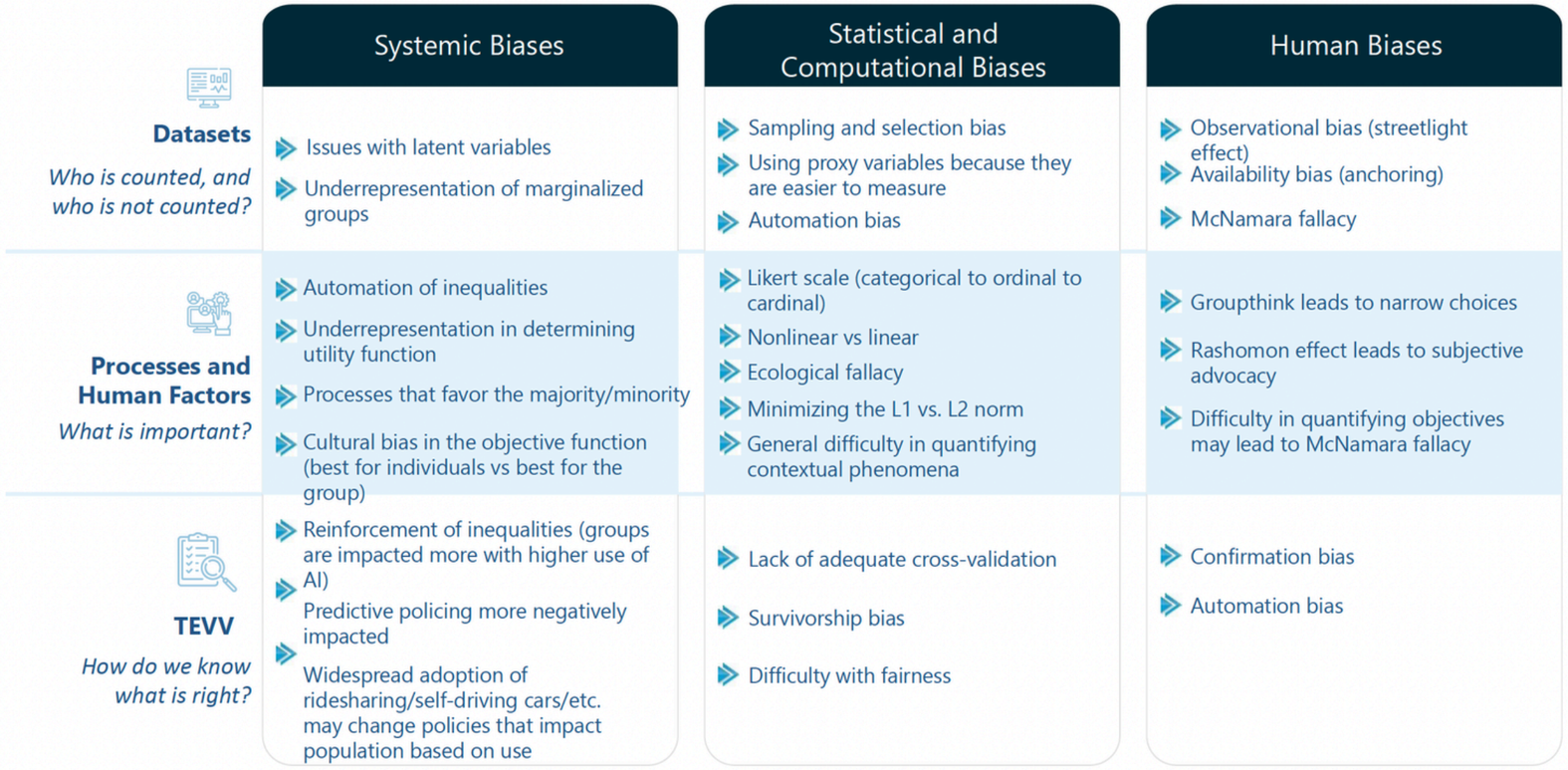


Fig. 5. How biases contribute to harms

Source: National Institute of Standards and Technology. (2022). Towards a standard for identifying and managing bias in artificial intelligence (NIST Special Publication 1270). https://doi.org/10.6028/NIST.SP.1270

DAIG DATA & AI GOVERNANCE PARTNERS

PART 7

Connecting the Dots

One integrated framework.

DAIG
DATA & AI GOVERNANCE
PARTNERS

The Data & AI Governance Framework

Six capabilities that together constitute a complete, operational governance system. These are not aspirational categories — they are the specific things you must build and operate.

01 **Foundations**

02 **Structure & Roles**

03 **Processes & Workflows**

04 **Measures & Feedback**

05 **Communication & Enablement**

06 **Frontline Governance**

USE CASE DRIVEN

Underpinned by Responsible AI & Data Ethics — Fairness, Transparency, Accountability, Safety & Human Oversight woven into every capability

DAIG DATA & AI GOVERNANCE PARTNERS

Capability 1: FOUNDATIONS

The strategic bedrock. Answers: why are we doing this, and what are we trying to achieve?

What you build

- Purpose and vision for governance
- Guiding principles that inform all decisions
- Current-state mapping of challenges across data and AI
- Alignment between governance objectives and business strategy
- Data & AI Friction Map (Sprint Exercise 1)
- Purpose statement (Sprint Exercise 2)
- 3–5 guiding principles (Sprint Exercise 3)

Sprint Workshop: Workshop 1 and 2

Why it matters

Without clear purpose and principles, governance becomes a set of rules without context. Teams won’t know why they’re doing it, executives won’t fund it, and practitioners won’t follow it.

DAIG DATA & AI GOVERNANCE PARTNERS

Capability 2: STRUCTURE & ROLES

The organizational backbone. Answers: who does what, who decides what, and how do governance bodies connect?

What you build

- Decision rights and accountability
- Integrated roles: Data Steward, Data Owner, Data Custodian, AI Product Owner, Model Risk Manager, AI Operations
- Target operating model (2–4 year vision)
- Minimum sustainable operating model (pilot-ready)
- Governance councils, working groups, escalation paths
- Responsibility mapping using integrated Data & AI cards

Sprint Workshop: Workshop 3

Why it matters

The most common governance failure: roles exist on paper but nobody knows what to do. The Sprint avoids this by starting with responsibilities (not roles), then mapping those responsibilities to people.

Critical design decision: Ensure data and AI governance roles are designed together, not separately. This prevents the fragmentation trap of building two parallel governance structures.

The minimum sustainable operating model is the key innovation: strip the ideal model down to the bare minimum needed for the pilot. Test it. Then expand.

DAIG DATA & AI GOVERNANCE PARTNERS

Capability 3: PROCESSES & WORKFLOWS

The operational engine. Answers: what specific processes do we need to govern CDEs and AI systems?

What you build

Default governance processes include:

- CDE data quality monitoring & remediation
- CDE metadata documentation
- AI risk classification & assessment
- AI lifecycle stage-gate controls
- Incident response procedures
- Access control workflows
- Change management procedures

Each process is mapped as a step-by-step workflow with swim lanes, decision points, triggers, and responsible parties.

Sprint Workshop: Workshop 4

Why it matters

Processes are where governance becomes operational. Without them, policies are just paper.

The Sprint uses Applied User Story Mapping to design processes collaboratively. Participants map who initiates each process, what triggers it, what steps are involved, who makes decisions, and what the outputs are.

AI-specific integration: AI risk assessment and lifecycle controls are mapped alongside CDE quality processes, with explicit integration points. Where do the data quality process and the AI risk assessment process share handoffs? The consolidated process map answers this.

Capability 4: MEASURES & FEEDBACK

The control tower. Answers: how do we know governance is working?

What you build

- Governance Scorecard with prioritized metrics:
  - Data quality: completeness, accuracy, consistency, timeliness
  - AI governance: fairness metrics, risk coverage, drift detection
  - Governance ops: stewardship activity, process compliance
  - Business impact: decision quality, cost reduction
- Control Canvas linking metrics → controls → owners → thresholds → escalation
- Measurement dashboard visible to executives
- Feedback loops for continuous improvement

Sprint Workshop: Workshop 5

Why it matters

What gets measured gets managed. Without a scorecard, governance is invisible to leadership and impossible to improve.

Governance KPIs should sit alongside business KPIs in executive dashboards — not in separate compliance reports. Make risk visible, measurable, and actionable for CFO, CMO, and CRO audiences.

The Control Canvas is the innovation here: for each metric, define what control is needed (preventive, detective, corrective), who owns it, how frequently it runs, what threshold triggers action, and what the escalation path looks like.

Capability 5: COMMUNICATION & ENABLEMENT

The adoption engine. Answers: how do we build understanding, capability, and a common language?

What you build

- Communication Blueprint: who needs to know what, through which channels, at what frequency
- Audience-specific messaging: executive (quarterly), management (monthly), operational (daily/weekly)
- Business Glossary: 20–30 critical terms with clear definitions (the common language)
- AI Literacy (or Fluency) program: what AI is, how it's used, what's expected of each role
- Training Roadmap: role-specific, format-specific, timeline-specific
- Change management strategy addressing the anthropological reality

Sprint Workshop: Workshop 6

Why it matters

Governance fails because people don't understand, accept, or adopt it. Communication and enablement are not nice-to-haves — they are existential requirements.

The Business Glossary is more impactful than it sounds. When departments use different definitions for the same term, every downstream process breaks.

Training alone is not enough — it must be accompanied by scenario-based practice (covered in Capability 6). This is why Communication & Enablement feeds directly into Frontline Governance.

DAIG DATA & AI GOVERNANCE PARTNERS

Capability 6: FRONTLINE GOVERNANCE

The ultimate goal. Answers: what does governance look like on a Tuesday afternoon for a data steward?

What you build

- Day-in-the-life scripts for each governance role
- Scenario-based testing protocols
- Prototype storyboards: step-by-step visual guides for testable governance
- Data governance scenarios: CDE quality issue detection, investigation, remediation, escalation
- AI governance scenarios: risk classification for new AI system, bias alert response, model drift handling
- Integration point: the prototype IS the training environment

Sprint Workshop: Workshop 7

Why this is the MOST CRITICAL capability

This is where the fire escape analogy becomes operational. You can write the best policies, assign the best roles, build the best processes — but if people never practice, they're lost when a real governance situation arises.

Frontline governance is governance that lives in daily operations, not in policy documents. It is the only kind of governance that actually works.

The Sprint's prototyping phase (Weeks 4–5) is designed specifically to test frontline governance. When testers work through realistic scenarios, they are simultaneously testing the design and training themselves. The prototype is the training environment.

This is the capability AI will never replace.

The framework is USE-CASE DRIVEN and ETHICS-UNDERPINNED

Two design principles that make this framework different from generic governance models:

USE-CASE DRIVEN

Capabilities are NOT built in the abstract. They are developed in service of specific, high-impact data and AI use cases.

Example: instead of designing a generic ‘data quality process,’ the Sprint designs a quality process for Customer Address Data (the CDE identified in Workshop 2). Instead of a generic AI risk framework, it designs risk classification for a specific credit scoring model.

This ensures immediate relevance and testability.

ETHICS-UNDERPINNED

Responsible AI and Data Ethics are not a separate module or ethical overlay. They are integrated design criteria woven into every capability:

- Fairness: built into measures, processes, and testing
- Transparency: built into communication and documentation
- Accountability: built into roles and operating model
- Safety & Human Oversight: built into frontline governance

Foundations	Structure	Processes	Measures	Communication	Frontline

DAIG DATA & AI GOVERNANCE PARTNERS

What is the Governance Sprint™?

A structured, workshop-driven, 5-week methodology that establishes Data and AI Governance capabilities through rapid design, prototyping, and testing — using real use cases, with real people, producing real outputs.

The formula:

7+	10	5	1	∞
Workshops	**Core Exercises**	**Weeks**	**Prototype**	**Embedding**
Structured, facilitated, decision-producing sessions	Reusable, proven exercise toolkit. Over the 7+ workshops we do 21 exercises.	Design through validated prototype	Tested with real users on real scenarios	Week 6+ scales through agile implementation

The power of the Sprint is that it’s a formula: a series of exercises spread across workshops over weeks. This formula acts as the red thread through everything you’ll learn in the next modules.

The Sprint is not a one-time event. It is a repeatable methodology for continuous governance expansion.

DAIG DATA & AI GOVERNANCE PARTNERS

The Governance Sprint™ — The Full Journey

7 workshops · 21 exercises · 5 weeks · from friction to validated prototype

WEEK 1	WEEK 2	WEEK 3	WEEK 4	WEEK 5
Foundations	Structure	Operationalise	Build & Test	Iterate & Validate

1 — Establishing Foundations
- Friction Map
- Purpose
- Principles

friction map
purpose v1.0
principles

2 — Bridge to Governance
- 10-for-10
- Action Board
- Roadmap

initiatives
shortlist
targets

3 — Governance Players
- Resp. Mapping
- Operating Model
- Roles Roster

roles
operating model
MVP roster

4 — Rules of the Game
- Data Process
- AI Risk Process
- Integration

3 process maps
integration
prototype scope

5 — Making It Stick
- Scorecard
- Toolkit
- Comm Blueprint

dashboard
templates
comm plan

6 — Engagement & Training
- Engagement
- Training
- Readiness

engagement plan
training matrix
RAG status

7 — Prototype Prep
- Test Scenarios
- Storyboard
- Build List

scenarios
storyboard
build list

PROTOTYPING
Build hi-fidelity interactive prototypes from Sprint artifacts

USER TESTING
5 testers
Data + AI scenarios
Feedback Wall

ITERATION WORKSHOP
Feedback synthesis
Sailboat + Strategic Q's
Concept refinement

VALIDATE & HANDOFF
Round 2 testing
Prototype adjustments
Sprint Outcomes Package

DESIGN PHASE — 7 workshops, 21 exercises

BUILD & TEST PHASE — prototype, test, iterate, validate

FOUNDATIONS	STRUCTURE & ROLES	MEASURES, COMMS & PREP	BUILD	VALIDATE

Confusion → Clarity → Methodology → Execution → Sustainability

DAIG DATA & AI GOVERNANCE PARTNERS

Key Data Governance artifacts

01 Business Glossary

The common language. 20–30 critical business terms with agreed definitions, owners, and synonyms.

02 Data Dictionary

Technical metadata for each attribute. Schema, types, validation rules, source systems.

03 Data Catalog & Lineage

Where data lives and how it flows. End-to-end traceability from source to consumption.

04 Classification Schema

Sensitivity tiers, regulatory tags (PII, PHI, financial), access categories for every asset.

05 DQ Dashboard

Live KPIs by domain: completeness, accuracy, consistency, timeliness — with thresholds and alerts.

06 Issue Register

Living log of identified quality issues, owners, root causes, status, remediation actions.

07 Operating Model

Steward, Owner, Custodian per data domain. Decision rights and escalation paths clarified.

08 Data Policies

Privacy, access, retention, security, sharing — the policy hierarchy, principles to procedures.

Key AI Governance artifacts

01 Classification Canvas

Categorize each AI system by type, risk tier, and regulatory scope. Gates entry into the rest of the process.

02 Risk Register

Living log of identified risks, likelihood, impact, mitigations, owners. Reviewed throughout the lifecycle.

03 TEVV Plan

Testing, Evaluation, Verification, Validation — methodologies, metrics, datasets, acceptance criteria.

04 Model Cards

Standardized documentation of model details, intended use, performance, limitations, ethical considerations.

05 Datasheets

Document dataset characteristics, collection methods, preprocessing, known biases, recommended uses.

06 RACI / RASCI Charts

Map AI lifecycle activities to roles — Responsible, Accountable, Supporting, Consulted, Informed.

07 Technical File

EU AI Act Annex IV — comprehensive compliance evidence; kept for 10 years post-market.

08 PMM Logs

Post-Market Monitoring — operational performance, drift, fairness, incidents, corrective actions.

DAIG
DATA & AI GOVERNANCE
PARTNERS

Upcoming Training: AI Governance Essentials

Thank you.

Let’s Connect The Dots Together

Build Data and AI Governance
in Weeks, Not Months.

Mathias Vercauteren

President, Data & AI Governance Partners

mathias@daigpartners.com | +32 468 258 947 | daigpartners.com