

Building Trust and Maturity in AI

Sep 04, 2026

ITU Training on AI Governance & Use Cases

Andrea Cartwright, Senior Manager, Responsible AI
acartwright@gsma.com

- 1. Defining Responsible AI (RAI)**
- 2. Accelerating Innovation**
- 3. The GSMA Responsible AI Roadmap**



What is responsible AI?

3

- Responsible AI is a set of principles that guide how AI is designed, built and used across sectors.
- It focuses on understanding the wider societal impact of AI and ensuring systems align with legal, ethical and stakeholder expectations.
- At its core, Responsible AI embeds these principles into AI ecosystems to reduce risks and harms while maximising positive outcomes.

Influential AI principles

The GSMA has established seven principles that aim to summarise the AI ethical principles set out by:



- 1 Fairness
- 2 Human agency and oversight
- 3 Privacy and security
- 4 Safety and robustness
- 5 Transparency and explainability
- 6 Accountability
- 7 Environmental wellbeing

Why responsible AI matters

In everyday terms, responsibility means:



Keeping people safe



Protecting privacy



Avoiding unfair or biased decisions



Making sure humans stay in control



Building trust so people feel comfortable using AI

“... ethics is non-negotiable. AI’s ethical implications are more complex than ever, and failing to embed ethics from the start carries risks that far outweigh mitigation costs.”

- Chief Data Officer, Telefonica

Risks of not operating responsibly



Misuse and
malicious use of AI



Inaccuracy, hallucinations
and misinformation



Lack of transparency
and explainability



Fairness, bias
and discrimination



Cybersecurity
vulnerabilities



Regulatory and
legal exposure



Loss of trust and
brand damage

Why the fight
against deepfakes
begins with trust,
not detection

How Artificial Intelligence,
IoT And Big Data Can Save
The Bees

Australian Regulator Investigates Grok AI for Generating
Sexualized and Exploitative Images

THE WAR ON DEEPPFAKES: HOW NATIONS ARE FIGHTING BACK

While Egypt enhances its technical defenses, South Korea is reinforcing the legal boundaries around deepfake misuse.

AI and Cancer: The Emerging Revolution

Air Canada ordered to pay customer
who was misled by airline's chatbot



Responsible AI and connectivity

01



Provides a foundation for trusted connectivity

02



Aligns with UN values and developmental goals

03



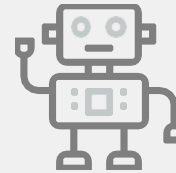
Strengthens global interoperability

04



Supports safe deployment of advanced AI, including agentic systems

05



Accelerates innovation while managing risk

06



Builds public and governmental trust

2. Accelerating Innovation

Challenging the myths

MYTH	RAI is just about compliance	MYTH	We already have governance
TRUTH	It's about building safe AI and earning trust	TRUTH	AI governance is different to data governance; AI introduces new risks
MYTH	RAI is a blocker that slows innovation	MYTH	The technology partner handles all the risk
TRUTH	Embedding AI principles reduces rework and prevents errors and speeds delivery	TRUTH	Responsibility can't be outsourced, organisations remain accountable for outcomes
MYTH	RAI is an IT issue	MYTH	Just needs doing once
TRUTH	It's an organisational capability requiring leadership, governance and culture; not a toolset	TRUTH	RAI is not a destination, but a continuous practice of learning and adaptation

Strong AI governance builds trust and unlocks innovation

In everyday terms, responsibility means:



Keeping people safe



Protecting privacy



Avoiding unfair or biased decisions



Making sure humans stay in control



Building trust so people feel comfortable using AI



... ethics is non-negotiable. AI's ethical implications are more complex than ever, and failing to embed ethics from the start carries risks that far outweigh mitigation costs.

Chief Data Officer, Telefónica

Responsibility drives real business value

01



Reduces operational and regulatory risk, protecting revenue and brand equity

02



Accelerates AI deployment at scale

03



Enables faster experimentation and innovations

04



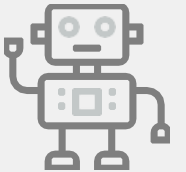
Strengthens partner and vendor alignment

05



Builds customer trust and adoption

06



Is essential for unlocking advanced and agentic AI use cases

3. Introducing the Responsible AI Roadmap

RAI Roadmap: a shared framework



OPERATOR LED

Developed by operators and AI experts, for operators (and partners), through global collaboration



ALIGNED WITH GLOBAL INTERNATIONAL STANDARDS

(ISO 42001, NIST AI RMF)



PRACTICAL AND MEASURABLE

Provides a clear path from Foundational to Advanced maturity



EXTENDS RAI

beyond internal operations to suppliers and partners



SELF-ASSESSMENT TOOL

for assessing readiness, benchmarking progress and guiding investment in RAI capabilities

Underpinned by years of GSMA engagement with the AI Taskforce

Building AI capability: Four stages, five dimensions

FOUR MATURITY LEVELS

Foundational →

Evolving →

Performing →

Advanced

FIVE CORE DIMENSIONS



01 Vision

- Aligns vision with executive sponsorship, risk appetite and regulatory alignment
- Creates a clear, shared direction



02 Operating model

- Sets governance and decision-making processes, clarifies how risks are mitigated, defines roles and responsibilities
- Considers the right RAI tooling to support consistent, scalable practice



03 Technical controls

- Data and model risk management set the foundation
- The control environment, technical guardrails, monitoring and clear incident response keep systems safe and predictable



04 Third-party ecosystem

- Third-party selection criteria and processes set the baseline for partners
- Third-party data protocols, monitoring, reporting and auditing ensure those partners stay aligned and accountable



05 Change management and communications

- Training builds capability and confidence across teams
- Culture, change management, and clear communication make AI understood and consistently applied

Linking AI Governance and Responsible AI (illustrative)

AI Governance	Responsible AI (RAI)
Structures & controls: Formal policies, oversight mechanisms and compliance requirements	Principles & practice: Behaviours, norms, and responsible design and deployment
Regulatory alignment: Meets legal, supervisory, and audit expectations	Ethical alignment: Focuses on fairness, transparency, accountability and societal impact
Risk frameworks: Organisational and systemic risk management	Human-centric risk: User impact, harm prevention, and trust
Lifecycle checkpoints: Defined stages for review and approval	Continuous responsibility: Ongoing monitoring and responsible behaviour across the lifecycle
Jurisdiction-specific: Varies by regulatory environment	Cross-industry consistency: Shared principles across operators, vendors and governments
Compliance focus: Ensures systems meet required standards	Trust & adoption: Builds confidence for safe, scalable deployment

Recommendations for implementing Responsible AI (RAI)



Engage
stakeholders



Assign clear
roles and
responsibilities



Conduct ethical
and risk
assessments



Define policies,
controls and
compliance



Invest in
training and
raising
awareness



Prioritise
inclusive
design and
diversity



Strengthen
governance and
technical
safeguards



Anticipate future
context

GSMA Responsible AI further reading

GSMA RAI Resources



Thank you!