GSMA

The GSMA Responsible AI Maturity Roadmap

September 2024

Maximising Value through Responsible AI: Methodology Overview

Implementing AI responsibly enables mobile operators to fully realise the economic potential of their AI initiatives, by building consumer trust, creating operational efficiencies and enhancing product quality.

The GSMA Responsible AI Maturity Roadmap, developed in partnership with the GSMA AI for Impact Taskforce and based on insights from McKinsey, provides companies with a structured framework to establish, monitor and enhance responsible AI practices. This tool allows organisations to assess their current level of responsible AI maturity, identify areas for improvement, and align their responsible AI strategies with their ambitions.

RAI maturity is measured across four levels—Foundational, Evolving, Performing, and Advanced—and is evaluated across five core dimensions: Vision, Operating Model, Technical Controls, Third-party Ecosystem, and Change Management and Communications. These dimensions are further divided into 20 sub-dimensions, ensuring a comprehensive assessment of all critical components required for responsible AI.

The roadmap also provides examples of evidence and proof-points that organisations can use to measure their level of responsible AI practices and track progress as their use of the technology evolves.

This asset forms part of a selection of documents that will enable organisations to better understand and implement responsible AI practices. Please also see the Step-by-Step Guide and Best Practice Tools.

How the roadmap was developed

The GSMA RAI Maturity Roadmap was rigorously reviewed and evaluated by 20+ experts:

18+

Interviews with RAI champions and experts to co-create and evaluate the framework

15+

Operators participated in the GSMA RAI sub group to review the maturity roadmap and align on design choices and framework

25+

Operators consulted as members of the GSMA AI for Impact Taskforce

Operators who worked on the roadmap

Champions

axiata

orange™

Telefónica

Contributors

e& etisalat and

kpn

Telefónica

orange™

TURKCELL

BT Group

true

stc

axiata

Singtel

telenor

TIM

vodafone

Globe

Telia Company

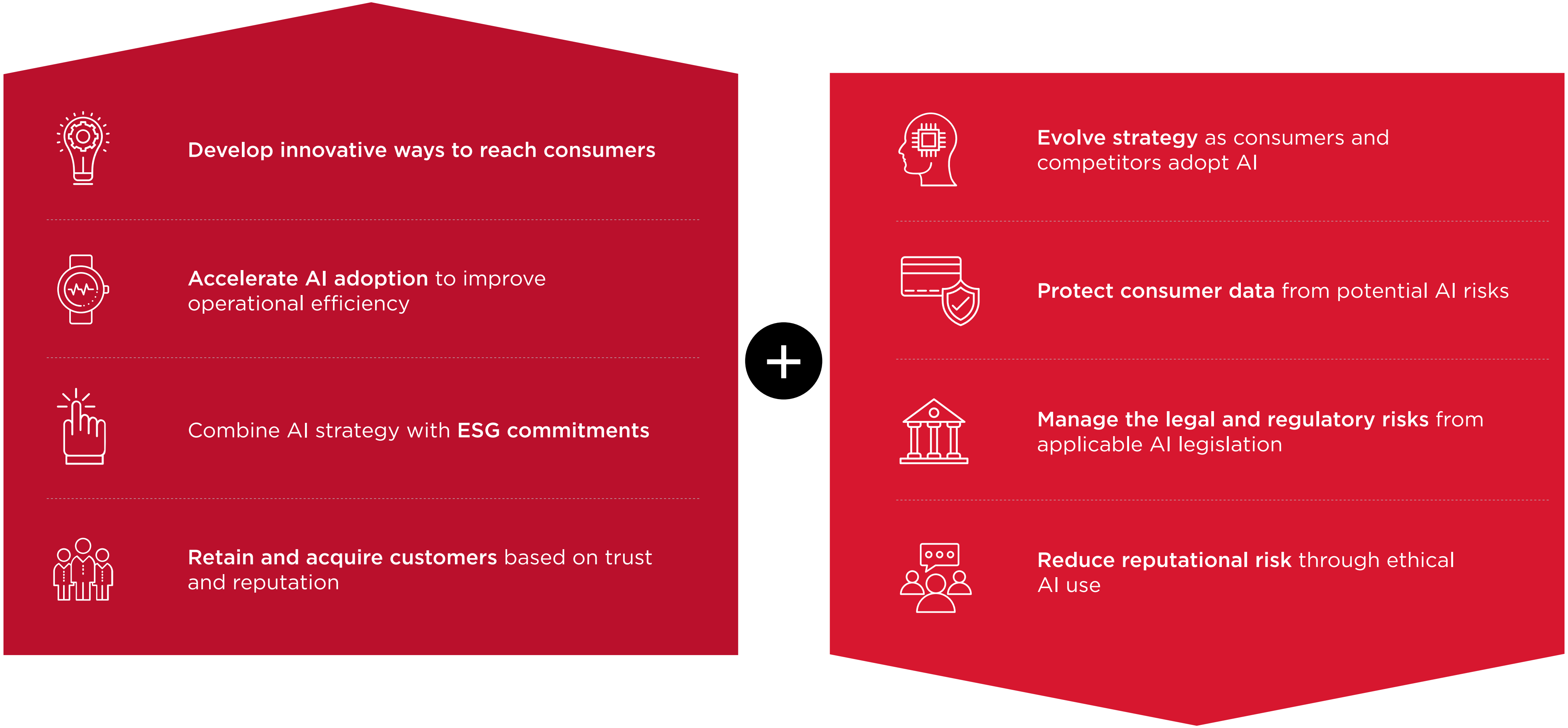
MTN

Contents

Importance of **Responsible AI**

Implementing AI responsibly will enable operators to realise maximum value from AI as not just value for operators but also value to others

NON-EXHAUSTIVE



Potential economic value from AI ambitions...

- **Develop innovative ways to reach consumers**
- **Accelerate AI adoption** to improve operational efficiency
- Combine AI strategy with **ESG commitments**
- **Retain and acquire customers** based on trust and reputation

+

... can be maximised through Responsible AI

- **Evolve strategy** as consumers and competitors adopt AI
- **Protect consumer data** from potential AI risks
- **Manage the legal and regulatory risks** from applicable AI legislation
- **Reduce reputational risk** through ethical AI use

The GSMA RAI Maturity Roadmap supports operators to fully realise their AI potential in alignment with their AI ambitions…

Operators vary in AI adoption and ambition levels

- Operators exhibit a broad spectrum of **AI ambition**, ranging from **early experimenters to advanced practitioners**
- Early experimenters often use **off-the-shelf third-party AI solutions to enhance operational efficiency**, while advanced practitioners leverage **AI at scale** across the entire organisation with **high-impact customer-facing use cases**

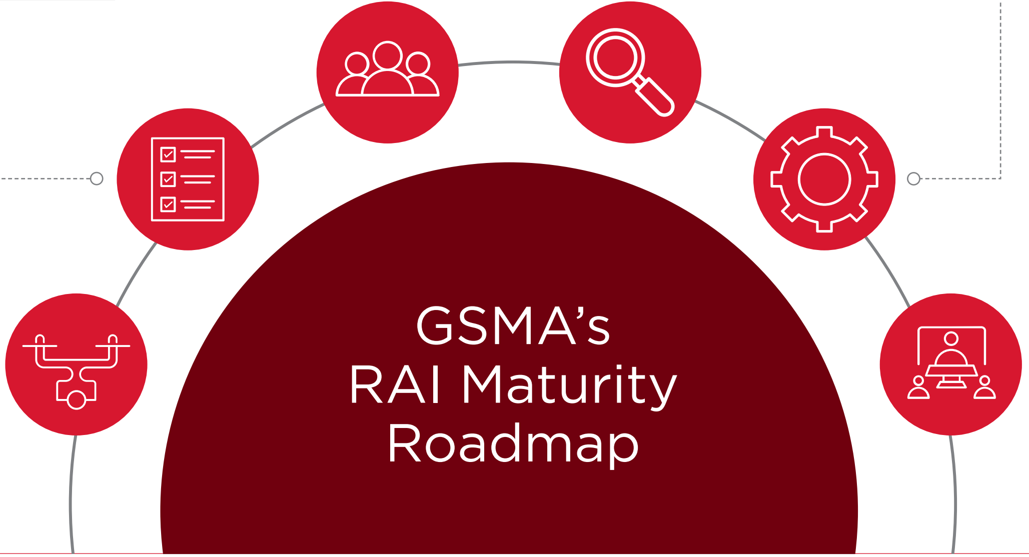
Expectations for RAI maturity will vary based on overall AI ambitions

- Maximising the **value of AI requires** not only capturing the upward potential (i.e. through high-impact use cases), but also **managing AI risks**
- As operators get started on adopting AI, it is essential **to first put key Foundational requirements** in place (e.g. RAI principles, key roles)
- **RAI expectations will further evolve** as AI adoption levels increase

RAI maturity roadmap describes necessary components at each level of RAI maturity

- The RAI maturity roadmap is an **overarching, industry-agnostic framework** that details the necessary **elements required to progress** in RAI maturity
- The roadmap provides **Telco-specific best practice examples** and **step-by-step guidance** to improve maturity in line with overall AI ambitions

… through various, unique components designed to **guide operators on their RAI journey**…



Adjusts the components of RAI to the overall AI maturity and ambition, helping balance the pace of innovation with appropriate guardrails

Encompasses all the essential components outlined in ISO 42001 and NIST frameworks, ensuring a roadmap that aligns with established standards

Extends beyond just risk management by detailing additional dimensions such as operating roadmap and third-party management

Establishes maturity levels to help assess their current RAI maturity and identify areas of improvement

Offers actionable recommendations by incorporating Telco-specific best practice examples

Provides an opportunity to showcase RAI maturity progress to internal leadership, the Board, and potentially the public

… integrating existing RAI frameworks and building on them with an **assessment and Telco-specific nuances**

NON EXHAUSTIVE AS OF MAY 2024

◌✓ SOMEWHAT MEETS CRITERIA ✓ MEETS CRITERIA ⊗ DOES NOT MEET CRITERIA

	FRAMEWORKS				MATURITY MODEL
Criteria: “The RAI maturity framework/ roadmap is…”	**ISO/IEC 42001** AI management system	**ISO/IEC 31050** Emerging risks Proactive approach	**ISO/IEC 23894** Artificial Intelligence Risk Management	**NIST AI RMF** NIST Artificial Intelligence Risk Management Framework	**GSMA RAI**
Underlying framework is not just risk-centric	✓ Covers dimensions beyond risk	⊗ Focus on risk and resilience	⊗ Focus on risk through AI lifecycle	✓ “Govern” slightly covers people and process	✓ Covers dimensions beyond risk
Documented process for conducting self-assessment	⊗ Controls and guidelines in place for external body to accredit	⊗ Controls and guidelines in place for external body to accredit	⊗ Controls and guidelines in place for external body to accredit	⊗ Subjective assessment without actionable tools	✓ Documented evidence, artifacts and certification
Includes maturity levels	⊗ N/A	⊗ N/A	⊗ N/A	◌✓ Tech Better builds on NIST AR RMF[1] Partially meets criteria	✓ Builds on frameworks and standards
Based on Telco considerations	⊗ Telco not included[2]	⊗ Broad industry application	⊗ Broad industry application	⊗ Broad industry application	✓ Exemplifies Telco-specific use cases

[1] TechBetter maturity model by Ravit Dotan is based on the NIST AI RFM (details in previous page)

[2] Mentions health, defence, transport, finance, employment and energy

Source: ISO, NIST, JCR EU Commission, TechBetter (Dotan et al.)

The GSMA RAI Maturity Roadmap allows operators to…

NON-EXHAUSTIVE

Identify and address gaps in their current processes by providing a structured framework to evaluate against and improve their RAI practices

Demonstrate their commitment to RAI practices that can help enhance reputation and build trust with stakeholders

Establish industry standards for developing, deploying, and monitoring AI systems, improving the overall performance, reliability, and safety of their solutions and help managing risks

Position themselves as a leader in RAI deployment by fostering a culture of continuous improvement and innovation

Deliver greater value to their clients by ensuring RAI, meeting client needs more effectively and building strong client relationships

The Roadmap **explained**

Aligning RAI maturity levels with AI ambitions is crucial to fully realise the value from AI safely

Relative RAI maturity progress: ● **Opportunity to improve** ● **On-track:** Only on-track use cases will capture full potential impact

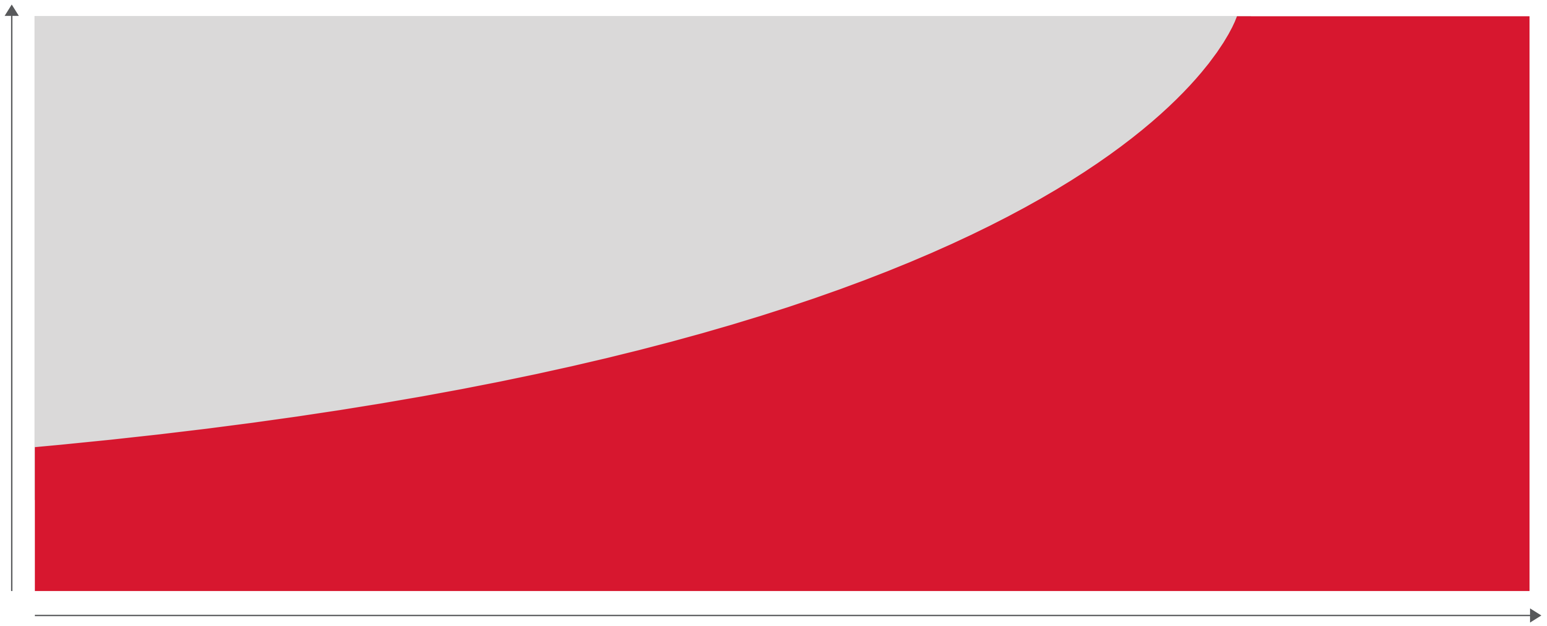
Organisational AI ambitions

Transforming
Additionally, use cases making autonomous decisions that affect customers are deployed

Formalising
Use cases in all domains can be safely deployed including human resources

Experimenting
Use cases with autonomous AI systems are deployed internally

Exploring
Internal use cases in some domains are deployed primarily by the use of off-the-shelf solutions



Ambitions are set organisation-wide, allowing **individual use cases to be deployed at different scales** (e.g. from pilots to full transformations)

Foundational
Initial awareness for RAI is established with four primary components in place

Evolving
Presence of structured processes and early integration of RAI

Performing
RAI principles are integrated with robust processes and governance

Advanced
RAI practices are deeply embedded into the culture with proactive management

Responsible AI (RAI) maturity levels

RAI maturity levels are defined across five core underlying dimensions, providing a framework to measure RAI maturity

1. Vision

Develop vision and principles for AI governance aligned with organisational values, strategic goals and regulatory alignment

2. Operating Model

Cultivate talent pool, proper team structure, ways of working and tooling solutions with robust risk management processes to implement and maintain AI governance across all organisational activities

3. Technical Controls

Strengthen technical risk management (with models, data, technology) to identify, monitor and mitigate risks, ensuring alignment with regulations and organisational risk appetite

4. Third-party Ecosystem

Establish partnerships with third parties in alignment with the organisation's risk strategy which involves monitoring, auditing and reporting activities

5. Change Management and Communications

Leverage training programmes, change management protocols, and internal and external communication strategies to operationalise comprehensive RAI practices

The five dimensions break down into 20 sub-dimensions in order to identify all the RAI components that need to be established

1 Vision

- 1.1 RAI principles
- 1.2 Executive sponsorship
- 1.3 Risk strategy (incl. risk appetite)
- 1.4 Regulatory alignment

2 Operating Model

- 2.1 Governance (oversight and decision-making)
- 2.2 Processes for identifying, assessing, and mitigating AI risks
- 2.3 Roles and responsibilities
- 2.4 RAI talent
- 2.5 AI development protocol
- 2.6 RAI tooling solutions

3 Technical Controls

- 3.1 Data management
- 3.2 Model risk management
- 3.3 Control environment (incl. technical guardrails)
- 3.4 Monitoring and incident response

4 Third-party Ecosystem

- 4.1 Third-party selection criteria and processes
- 4.2 Third-party data management protocols
- 4.3 Third-party monitoring, reporting and auditing

5 Change Management and Communications

- 5.1 Training
- 5.2 Culture and change management
- 5.3 Communication

Detailed descriptions of the sub-dimensions of the **RAI Maturity Roadmap**

DIMENSIONS	SUB-DIMENSIONS	DESCRIPTION
1. Vision	1.1 RAI principles	• Establish RAI principles based on international standards and best practices
	1.2 Executive sponsorship	• Ensure that key stakeholders, including executive sponsors, are aligned with and supportive of the RAI vision and principles
	1.3 Risk strategy (incl. risk appetite)	• Develop a risk strategy that complements the organisation's risk appetite
	1.4 Regulatory alignment	• Ensure alignment to all relevant legal and regulatory requirements governing AI, including compliance with applicable local and global laws (e.g., data privacy regulations, industry-specific standards)
2. Operating Model	2.1 Governance (oversight and decision-making)	• Establish governance that provides oversight, and guides decision-making and accountability for RAI implementation
	2.2 Processes for identifying, assessing, and mitigating AI risks	• Establish processes to identify, assess, and mitigate AI-related risks that involves defining and leveraging KRIs and existing risk management frameworks
	2.3 Roles and responsibilities	• Define roles and responsibilities (involves RAI champions, ethics officers, RAI experts, etc.) to manage RAI transparently and effectively across the organisation
	2.4 RAI talent	• Identify and recruit/upskill individuals to possess the technical skills, ethical awareness and commitment to implement and maintain RAI within the organisation
	2.5 AI development protocol	• Adopt a systematic and repeatable AI development process (incl. practices like documentation, customer testing, participatory design, and the "RAI by design" approach to incorporate risk management early in the design phase
	2.6 RAI tooling solutions	• Deploy tooling solutions to ensure AI governance, including an AI use case registry/registries (as appropriate based on how risk is managed by the organisation) to document and track AI use cases as applicable

Detailed descriptions of the sub-dimensions of the **RAI Maturity Roadmap**

DIMENSIONS	SUB-DIMENSIONS	DESCRIPTION
3. Technical Controls	3.1 Data management	• Ensure the use of quality, trustworthy data that underpins decision-making (e.g., minimise malicious use and security threats through consideration of sensitive variables within the data such as race or ethnicity)
	3.2 Model risk management	• Establish model risk management practices to address risk issues (e.g., for inaccurate output, model drift, algorithmic bias)
	3.3 Control environment (incl. technical guardrails)	• Develop a control environment with technical guardrails and controls to ensure compliance with applicable regulations (e.g., EU AI Act)
	3.4 Monitoring and incident response	• Monitoring of KRIs (in real-time, as required) for oversight and improvement of AI systems once deployed, along with incident response plans to manage and respond to failures in AI systems
4. Third-party Ecosystem	4.1 Third-party selection criteria and processes	• Develop specific criteria, requirements, and processes within formal selection processes for third-party partners based on RAI principles and practices
	4.2 Third-party data management and protocols	• Establish protocols and guidelines for third-party partners, defining activities such as responsible data handling and management
	4.3 Third-party monitoring, reporting and auditing	• Implement processes for ongoing monitoring, auditing and reporting of third-party performance
5. Change Management and Communications	5.1 Training	• Develop and implement comprehensive training programmes to educate/upskill employees about AI regulations and RAI practices to raise awareness
	5.2 Culture and change management	• Foster an organisational culture that values and prioritises RAI principles, and execute change management with incentives in-place to promote ethical behaviour and accountability
	5.3 Communication	• Develop communication channels (incl. feedback) to ensure that employees, customers, and partners are informed about the organisation's commitment to RAI (e.g., virtual spaces community)

Summary of the maturity roadmap across dimensions and maturity levels

RAI practices are deeply embedded into the culture with proactive management

RAI maturity levels

DIMENSIONS	FOUNDATIONAL	EVOLVING	PERFORMING	ADVANCED
1 Vision	***Established RAI principles (1.1)*** **with initial recognition from leadership,** setting groundwork for future sponsorship with **initial awareness of regulations and risk strategy**	Efforts underway to adopt **RAI principles across departments** with initial steps towards stakeholder alignment, risk strategy identification and regulatory alignment	**RAI principles are starting to be integrated into operations** with **risk strategy defined and risk appetite outlined** (in alignment with applicable regulations)	**RAI principles embedded deeply in the organisation** in line with vision, strong **support from executive sponsors** through investments, and a mature **risk strategy regularly updated**
2 Operating Model	**Initial understanding of the need for formal governance structures** with ***essentials roles defined (2.3)*** and ***basic registry/registries for tracking AI use cases established (2.6)***	Initial **governance efforts with accountability mechanisms, basic risk management** tailored to risk severity, and **preliminary recruitment efforts** in place	**AI governance in place with pool of RAI talent,** risk management process applied for most use cases and **AI governance platform established** with limited functionality	**Governance with oversight and strategic decision-making** supported by defined roles, **'RAI by design' practices** and **AI governance platform across the enterprise**
3 Technical Controls	**Technical controls in early stages** with existing ones being ad-hoc and manual with a scope of further development and automation	**Controls are evolving** with preliminary processes for model risk management **(MRM), basic guardrails and incident response plans** starting to be developed	**Control environment developed** with **MRM practices and technical guardrails,** incl. initial efforts to monitor KRIs (in real-time as required), with **documented response plans**	**Effective controls in place** for managing AI risks with comprehensive data integrity protocols, **advanced MRM, automated monitoring of KRIs** and **regularly updated response plan**
4 Third-party Ecosystem	**Established basic RAI-specific criteria (4.1) for selecting third-party partners,** but selection processes are still ad-hoc with protocols in early stages	**Detailed selection criteria documented,** with basic protocols on third-party data management being developed and **siloed monitoring of applicable third-party partners**	**Criteria are regularly updated** for third-party partner selection, with **protocols for data handling** supported by **monitoring and auditing at consistent intervals**	**Existing and future contracts include RAI-specific clauses** with **continuous monitoring and auditing processes** (in real time, as required) for evaluating third-party performance
5 Change Management and Communications	**Initial thinking** started **towards developing training programmes** with **awareness for building culture** around RAI principles	**Beginning basic RAI training** and fostering a RAI culture with early efforts in **developing communication channels**	**Optional training programmes** with a mandate for key roles established, **change management incorporated into ongoing operations,** and **internal feedback mechanisms** in place	**Mandatory RAI training** with a **deeply ingrained RAI culture** valuing mentorship, and highly effective **internal and external communication and feedback mechanisms**

Red text indicates minimum requirements across four essential sub-dimensions needed to reach a foundational level of responsible AI maturity

Operationalisation of the **GSMA Responsible AI Maturity Roadmap**

Proposed approach to using the **RAI maturity roadmap**

Approach may vary slightly for each organisation

NON-EXHAUSTIVE

1 **Decide scope of assessment:** Identify whether assessment will be done across the entire organisation, at the Opco-level, or by function, to achieve a consistent evaluation

2 **Determine overall AI ambitions:** Assess and identify overall AI ambitions for the next year to set expectations for RAI maturity target state

3 **Identify evaluator:** Determine whether the evaluation will be conducted internally or by a third-party

4 **Conduct assessment with key stakeholders:** Complete the RAI maturity assessment with a select group of stakeholders (e.g., key point of contact[1], leads from Legal, Compliance, Privacy Risk, Data etc.)

5 **Outline action plan:** Compare current state RAI maturity with target state (determined in step 2) and relevant industry averages, leveraging step-by-step guidance and best practice examples to outline tactical next steps and recommendations for improving RAI practices within the organisation in line with overall AI ambitions

Assessment methodology

a. Identify key stakeholders involved in the RAI maturity assessment *(will vary for each operator)*

b. Review descriptions for each sub-dimension across the maturity levels (Foundational to Advanced)

c. Evaluate alignment of current RAI practices with descriptions of each sub-dimension, considering existing processes, technologies, and behaviours within the organisation

d. Assign maturity levels (Foundational to Advanced) to each sub-dimension based on the evaluation of current RAI practices, leveraging evidence, quantifiable proof-points (KPIs) and follow-up interviews where applicable

e. Aggregate RAI maturity levels for each sub-dimension (using the mean of all sub-dimension maturity levels) to determine current RAI maturity at the dimension and organisation level

f. Conduct RAI maturity assessment at consistent intervals (e.g., every year) or during significant shift in organisation-wide AI strategy to re-evaluate progress

[1] Example key points of contact include Head of Responsible AI, Head of AI, Global Head of Privacy by Design etc.

Evidence will strengthen evaluation, complementing stakeholder interviews for enhanced reporting

Assessment approach

1. Assess current practices against RAI maturity roadmap (i.e., review descriptions for sub-dimensions across maturity levels)
2. Conduct interviews (as needed) to validate assessment of current RAI practices
3. Complement interviews by reviewing evidence to verify maturity of specific sub-dimensions
4. To further validate the maturity of specific sub-dimensions, use quantifiable proof points (i.e., KPIs)

Note: Current set of supporting evidence is streamlined to minimise operational burden, but additional evidence can be requested as needed

Supporting evidence across RAI maturity levels *(not exhaustive)*

DIMENSIONS	FOUNDATIONAL	EVOLVING	PERFORMING	ADVANCED
1. Vision	1.1 Published RAI principles		1.3 Risk appetite statement	1.2 Allocation of resources and budget to RAI efforts (e.g., budget plans)
2. Operating Model	2.3 Defined key roles and responsibilities 2.6 Use case registry/ registries (e.g., in Excel)	2.2 Set of defined KRIs (e.g., dashboard) 2.4 Job descriptions for RAI talent	2.2 Documented RAI processes 2.2 Risk-based use case prioritisation framework 2.5 Standardised AI development protocol (incl. "RAI by design")	2.1 AI governance forum TOR (terms of reference)
3. Technical Controls		3.1 Reports/ guidelines on data quality checks and validation processes 3.4 Incident response plans	3.3 Library of controls	3.2 Model risk management, practices 3.4 Monitoring dashboard and/or logs
4. Third-party Ecosystem	4.1 RAI third-party evaluation criteria		4.1 Guidance on required RAI contract clauses 4.3 Audit reports and compliance assessments	
5. Change Management and Communications		5.1 RAI training programmes	5.2 Change management plans	

Examples of evidence for **enhanced reporting across maturity levels**

NON-EXHAUSTIVE

Responsible AI (RAI) maturity level ○ Foundational ◐ Evolving ● Performing ◉ Advanced

DIMENSIONS	SUB-DIMENSIONS	EVIDENCE	DESCRIPTION
1. Vision	1.1 RAI principles	○ Published RAI principles	• Documented commitment to RAI through the publication of RAI principles
	1.3 Risk strategy (incl. risk appetite)	● Risk appetite statement	• Formal statement outlining the org.'s tolerance (quantitatively or qualitatively expressed) for AI risk in pursuing its AI ambitions
	1.3 Risk strategy (incl. risk apetite)	● Library of core value drivers	• Specific levers through which the org.'s AI initiatives could create value, aligned with the core RAI principles
	1.2 Executive sponsorship	◉ Allocation of resources and budget to RAI efforts (e.g., budget plans)	• Financial commitment to RAI demonstrated through dedicated budget allocation and resource plans
2. Operating Model	2.3 Roles and responsibilities	○ Defined key roles and responsibilities	• Descriptions of essential roles and reporting structures, defining overview of responsibilities for each role
	2.6 RAI tooling solutions	○ Use case registry/registries (e.g., in Excel)	• Registry/registries for documenting and tracking details of AI use cases (e.g., scope, value, costs, risks)
	2.2 Processes for identifying, assessing, and mitigating AI risks	◐ Set of defined KRIs (e.g., dashboard)	• Pre-defined set of key risk indicators (KRIs) that identify and track potential AI risks (e.g., through a dashboard)
	2.4 RAI talent	◐ Job descriptions for RAI talent	• Job postings or internal descriptions outlining the skills and experience required for RAI-related roles
	2.2 Processes for identifying, assessing, and mitigating AI risks	● Documented RAI processes	• Written procedures/policies outlining the specific steps involved in identifying, assessing, and mitigating AI-related risks
	2.2 Processes for identifying, assessing and mitigating AI risks	● Risk-based use case prioritisation framework	• Use case evaluation framework includes criteria that prioritises use cases based on potential AI risks and alignment with the org's risk appetite
	2.5 AI development protocol	● Standardised AI development protocol (incl. "RAI by design")	• AI development lifecycle protocols are standardised and documented, including established practices such as the "RAI by design" approach
	2.1 Governance (oversight and decision-making)	◉ AI governance forum TOR (terms of reference)	• Official document outlining the purpose, scope, members, and operational guidelines for the AI governance forum

[1] The role is not equivalent to an FTE; instead, one person can hold multiple roles

Examples of evidence for **enhanced reporting across maturity levels** (cont.)

NON-EXHAUSTIVE

Responsible AI (RAI) maturity level ⚪ Foundational ⚫ Evolving 🔴 Performing 🟤 Advanced

DIMENSIONS	SUB-DIMENSIONS	EVIDENCE	DESCRIPTION
3. Technical Controls	3.1 Data management	⚫ Reports/guidelines on data quality checks and validation processes	• Documentation (e.g., reports, guidelines, SOPs) outlining data quality objectives (DQOs) and procedures for verifying and validating data
	3.4 Monitoring and incident response	⚫ Incident response plans	• Documented plan outlining procedures for containing, mitigating, and recovering from AI incidents
	3.3 Control environment (incl. technical guardrails)	🔴 Library of controls	• Collection of documented controls (e.g., technical, procedural, cultural) that can mitigate different AI risks
	3.2 Model risk management	🟤 Model risk management practices	• Clear policies and procedures for model development, validation, implementation, and monitoring
	3.4 Monitoring and incident response	🟤 Monitoring dashboard and/or logs	• System that displays data streams (logs) or visualisations (dashboard) to track KRIs and potential AI risks, in real-time if applicable
4. Third-party Ecosystem	4.1 Third-party selection criteria and processes	⚪ RAI third-party evaluation criteria	• Initial set of third-party selection/evaluation criteria specific to RAI
	4.1 Third-party selection criteria and processes	🔴 Guidance on required RAI contract clauses	• Guidelines outlining the clauses that should be part of third-party contracts to ensure appropriate adherence to RAI practices
	4.3 Third-party monitoring, reporting and auditing	🔴 Audit reports and compliance assessments	• Documented reviews and assessments of third-party partners' RAI practices and protocols
5. Change Management and Communications	5.1 Training	⚫ RAI training programmes	• Internal training material used to educate employees on RAI practices (e.g., RAI principles, regulations)
	5.2 Culture and change management	🔴 Change management plan	• Formal plan detailing the strategy to increase employee adoption of RAI practices

Proof points can showcase RAI maturity progress to key stakeholders and can further complement assessment findings, for example:

NON-EXHAUSTIVE

Role of proof points

Proof points can be used to **showcase the progress in RAI maturity** to executive-level or external stakeholders

These could be **tracked regularly** in a **dashboard by the operator**

Additionally, while proof points do not directly impact the RAI maturity assessment, they can **complement findings gathered from interviews and evidence**

DIMENSIONS	PRIORITISED PROOF POINTS	PROOF POINT MEASURES THE PROPORTION OF...
1. Vision	1.2 **% RAI** investment	**Investment in RAI-specific initiatives, projects, and resources** compared to total AI investment
2. Operating Model	2.4 **% of employees** with RAI skills	**Employees who possess the necessary skills** related to RAI (measured by managers/HR) compared to all employees
3. Technical Controls	3.3 **% of automated controls** in place	**Technical controls that have been automated** compared to the total number of controls in place
4. Third-party Ecosystem	4.1 **% of third-party contracts** with RAI clauses	**Third-party contracts** that include **all required RAI clauses per org. guidelines** compared to all applicable third-party contracts
5. Change Management and Communications	5.1 **% of employees** who have completed RAI training	**Employees** who have successfully **completed RAI-specific training programmes** compared to all employees

For more information on the GSMA Responsible AI Maturity Roadmap, visit our website, watch the video or view the Step-by-Step Guide and Best Practice Tools documents.

You can also access the online tool to determine your organisations Responsible AI Maturity level here.