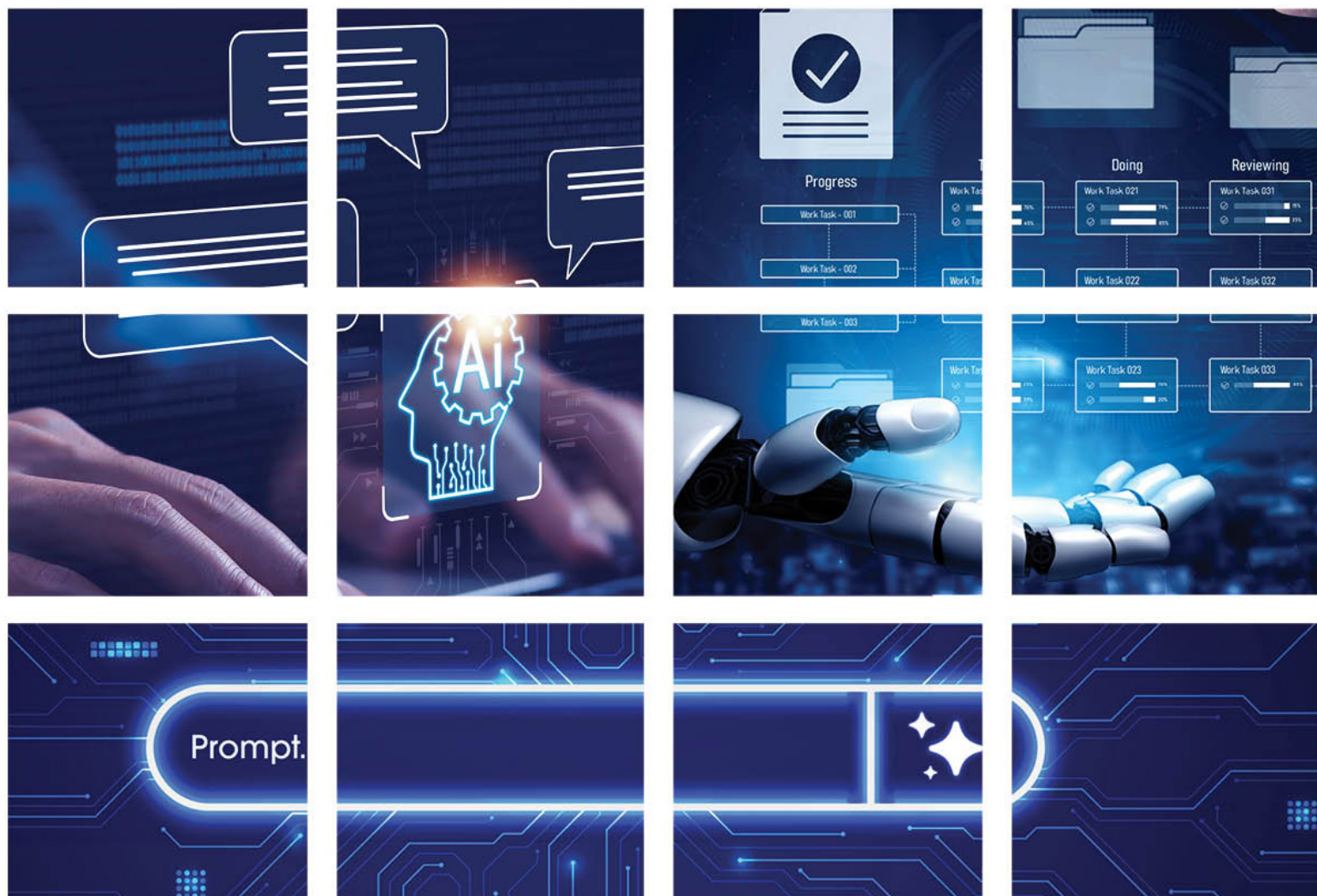


Collaborative artificial intelligence (AI) frameworks and preparedness diagnostic:

A practical guide for policy-makers and regulators



Acknowledgements

This publication was prepared by Ms Miriam Stankovich, Senior ICT Consultant, under the direction of the Regulatory and Market Environment Division of the ITU Telecommunication Development Bureau (BDT).

Disclaimer

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the International Telecommunication Union (ITU) or of the ITU secretariat concerning the legal status of any country, territory, city, or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned. Errors and omissions excepted; the names of proprietary products are distinguished by initial capital letters.

All reasonable precautions have been taken by ITU to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader.

The opinions, findings and conclusions expressed in this publication do not necessarily reflect the views of ITU or its membership.

ISBN

978-92-61-43391-8 (Electronic version)

978-92-61-43401-4 (EPUB version)



Please consider the environment before printing this report.

© ITU 2026

Some rights reserved. This work is licensed to the public through a Creative Commons Attribution-Non-Commercial-Share Alike 3.0 IGO license (CC BY-NC-SA 3.0 IGO).

Under the terms of this licence, you may copy, redistribute and adapt the work for non-commercial purposes, provided the work is appropriately cited. In any use of this work, there should be no suggestion that ITU endorse any specific organization, products or services. The unauthorized use of the ITU names or logos is not permitted. If you adapt the work, then you must license your work under the same or equivalent Creative Commons licence. If you create a translation of this work, you should add the following disclaimer along with the suggested citation: "This translation was not created by the International Telecommunication Union (ITU). ITU is not responsible for the content or accuracy of this translation. The original English edition shall be the binding and authentic edition". For more information, please visit <https://creativecommons.org/licenses/by-nc-sa/3.0/igo/>

Collaborative artificial intelligence (AI) frameworks and preparedness diagnostic:

**A practical guide for
policy-makers and regulators**



Table of contents

Acknowledgements	ii
Foreword	vi
Abbreviations and acronyms	vii
1 Introduction: Building preparedness through collaborative AI frameworks	1
1.1 From principles to enforceable obligations	1
1.2 Why collaborative frameworks are becoming indispensable	2
1.3 Objectives and structure of this integrated guide	3
2 Global overview of AI laws and regulations: Implications for collaborative frameworks (2023-2026).....	4
2.1 AI fundamentals: why they matter for preparedness	4
2.2 The evolution and diversity of AI regulatory approaches.....	5
2.3 European Union: The Artificial Intelligence Act (AI Act) and its collaborative AI requirements	9
2.4 Americas: diverse regulatory models and emerging convergence	11
2.5 Asia-Pacific: hybrid approaches from binding rules to soft-law toolkits	13
2.6 Africa and Arab States: building from data and digital foundations.....	15
2.7 Commonwealth of Independent States: state-led digital transformation, strategic coordination and uneven regulatory maturation	16
2.8 Cross-cutting trends and their implications for collaborative governance	17
3 Concept, purpose and methodology of a practical AI preparedness diagnostic	20
3.1 What is AI preparedness for policy-makers and regulators, and why does it matter?	20
3.2 The eight policy-relevant preparedness dimensions	25
3.3 Step-by-step methodology for performing the diagnostic	26
4 Diagnostic components by preparedness dimension: Questions, maturity levels and indicators.....	31
4.1 Dimension 1: Vision and strategic alignment.....	33
4.2 Dimension 2: Governance and institutional preparedness for collaborative AI frameworks	35
4.3 Dimension 3: Digital and computing infrastructure	37
4.4 Dimension 4: Data governance and data ecosystems	38
4.5 Dimension 5: Talent, skills and institutional capabilities.....	40
4.6 Dimension 6: Innovation, competition and procurement	42
4.7 Dimension 7: Ethics, trust and societal preparedness	43
4.8 Dimension 8: Implementation, supervision and enforcement preparedness	45

4.9 Overall preparedness.....	47
5 Conclusion: Collaborative frameworks and preparedness diagnostics as twin pillars of AI governance	48
Annex I: Illustrative application of the AI preparedness diagnostic: the case of Novara	50
Annex II: From vision to implementation – a practical roadmap for national AI collaborative governance.....	60

List of box, figures and table

List of box

Box 1: Use cases of AI preparedness diagnostics to implement policies and regulations	22
---	----

List of figures

Figure 1: AI systems.....	5
Figure 2: Artificial Intelligence strategies and policies, by region, 2021–2025	6
Figure 3: Illustrative AI collaborative framework architecture in a European Union Member State under the AI Act	10
Figure 4: Seven features shaping the AI regulatory landscape	18
Figure 5: The eight policy-relevant preparedness dimensions	26
Figure 6: AI preparedness assessment – six-step process.....	27
Figure 7: Maturity levels.....	33

List of table

Table 1: Comparative overview of regional AI collaborative frameworks and regulatory preparedness.....	6
--	---

Foreword



Artificial intelligence (AI) technologies are evolving at a rapid pace, becoming increasingly part of our everyday life. This evolution is creating both opportunities and challenges. While AI can support innovation, efficiency and service delivery, it also raises complex governance issues that cut across institutional mandates, sectors and jurisdictions. No single authority can address these challenges in isolation. An effective, collaborative AI framework therefore requires coordinated action across public institutions, regulators and stakeholders.

The guide places particular emphasis on the enabling role of digital and telecommunication infrastructure. AI systems depend on connectivity, data ecosystems and computing resources. Correspondingly, information and communication technology (ICT) regulators have a critical role in supporting secure, resilient and inclusive digital environments for AI deployment.

The guide has two complementary objectives. First, it seeks to update and provide a more in-depth analysis of collaborative AI frameworks, reflecting legal, institutional and policy developments from 2023 to 2026. Second, it introduces a practical AI preparedness diagnostic to help national and subnational authorities assess whether the institutional, infrastructural, legal, technical and human capacities needed to operationalize these frameworks are in place.

The methodology presented in this guide is intended to be used in different countries and institutional contexts. It offers policy-makers and regulators practical steps to strengthen collaboration, build capacity and ensure that AI systems are deployed in a way that is safe, inclusive and aligned with sustainable development objectives. AI governance will continue to evolve. Preparedness should therefore be understood as a continuous process, requiring regular assessment, institutional learning and adaptation.

This work builds on our ongoing efforts to support our Member States, in assessing their readiness and in building foundational telecommunication/ICT infrastructure as enablers for AI adoption, in line with Resolution 91 (Baku, 2025) of the World Telecommunication Development Conference on Artificial intelligence technologies in telecommunication development. I am confident that this guide will contribute to support countries to strengthen governance, enhance coordination, and ensure that AI is deployed in a manner that is trustworthy, inclusive and aligned with sustainable development priorities.

Dr Cosmas Luckyson Zavazava

Director of the Telecommunication Development Bureau
International Telecommunication Union

Abbreviations and acronyms

Abbreviation	Description
ACCC	Australian Competition and Consumer Commission
AESIA	Spanish Agency for the Supervision of Artificial Intelligence
AGI	Artificial general intelligence
AI	Artificial intelligence
AIDA	Artificial Intelligence and Data Act
ANATEL	Agência Nacional de Telecomunicações / National Telecommunications Agency of Brazil
ANI	Artificial narrow intelligence
ASEAN	Association of Southeast Asian Nations
BDT	Telecommunication Development Bureau
CIS	Commonwealth of Independent States
DPA	Data Protection Authority
DPDP	Digital Personal Data Protection Act
EU	European Union
GDPR	General Data Protection Regulation
GPAI	Global Partnership on Artificial Intelligence
GPU	Graphics processing unit
HPC	High-performance computing
ICT	Information and communication technology
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IMF	International Monetary Fund
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ITU	International Telecommunication Union
LGPD	Lei Geral de Proteção de Dados Pessoais / General Personal Data Protection Law of Brazil
OECD	Organization for Economic Co-operation and Development
POPIA	Protection of Personal Information Act of South Africa
SMEs	Small and medium-sized enterprises
UN	United Nations

(continued)

Abbreviation	Description
UNCTAD	United Nations Conference on Trade and Development
UNDP	United Nations Development Programme
UNESCO	United Nations Educational, Scientific and Cultural Organization
WTDC-25	World Telecommunication Development Conference 2025

1 Introduction: Building preparedness through collaborative AI frameworks

1.1 From principles to enforceable obligations

Artificial intelligence (AI) has become part of everyday collaborative governance. ICT regulators oversee AI-assisted network management and spectrum optimization; financial supervisors tackle AI-driven credit scoring and algorithmic trading; health authorities review AI-based diagnostics and triage tools; tax agencies rely on anomaly-detection models to identify fraud; and law-enforcement bodies experiment with predictive policing and facial recognition.¹ In the early 2020s, most jurisdictions responded with non-binding instruments, such as national AI ethics principles, high-level guidelines and voluntary frameworks. While these documents helped to set expectations, they often provided only limited practical guidance for regulators and deployers. Since 2023, a second wave of AI governance regulatory frameworks has emerged, characterized by binding laws and regulatory measures in the European Union,² Canada,³ Brazil,⁴ China (with binding rules on algorithmic recommendation, deep synthesis and generative AI services), Japan (with the AI Promotion Act), the Republic of Korea (AI Basic Act) and numerous federal states in the United States of America, including Colorado and California.⁵

This shift from “soft law” (quasi-legal, non-binding instruments such as strategies, recommendations or guidelines) to “hard law” (binding legal frameworks) has entailed several consequences. Obligations increasingly apply directly to actors across the AI value chain, developers, providers, deployers, importers and distributors, rather than remaining purely aspirational. Supervisory architectures must therefore adapt to oversee AI systems in a risk-based, technically informed manner. Coordination requirements are also increasing: AI regulation intersects with data protection, including the European Union General Data Protection Regulation (GDPR),⁶ the General Personal Data Protection Law of Brazil (LGPD),⁷ the Protection of Personal Information Act (POPIA) in South Africa, the Digital Personal Data Protection Act in India; cybersecurity; consumer protection; telecommunications; competition law; sector-specific regulation and human rights law. For regulators and policy-makers, the central challenge is therefore not simply to “have an AI strategy” but to ensure that legal frameworks, institutions, tools and capacities are aligned to ensure the effective, credible and proportionate governance of AI systems.

This guide adopts a comprehensive view of AI governance instruments, encompassing both soft law instruments (such as national AI strategies, policies, ethical frameworks and guidelines) and hard law instruments (including binding laws, regulations and enforceable standards).

¹ International Telecommunication Union (ITU), AI for Good, artificial Intelligence standardization and related foundational work, <https://www.itu.int/en/ITU-T/AI/Pages/default.aspx>

² European Commission, Regulatory framework for artificial intelligence: AI Act, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

³ Parliament of Canada, Bill C-27, Digital Charter Implementation Act, 2022, first reading, <https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading>

⁴ Oxford China Policy Lab, Brazil: striving for Latin American leadership in AI, <https://ocpl.substack.com/p/brazil-striving-for-latin-american>

⁵ International Association of Privacy Professionals (IAPP), Global AI Law and Policy Tracker: highlights and takeaways, <https://iapp.org/news/a/global-ai-law-and-policy-tracker-highlights-and-takeaways>

⁶ GDPR.eu., General Data Protection Regulation resources, <https://gdpr.eu>

⁷ Government of Brazil, Lei Geral de Proteção de Dados Pessoais, Lei No. 13.709/2018, http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

In practice, countries typically follow an evolutionary pathway, in which early-stage strategies and policy frameworks define national priorities, principles and institutional roles, and are subsequently translated into binding legal and regulatory measures as implementation capacity matures.

To support comparative analysis, this guide considers the full spectrum of instruments and, where relevant, enables assessment of the proportion of countries adopting different types of instruments, providing an indication of global maturity and regulatory convergence.

Developed in line with WTDC-25 Resolution 91 (Baku, 2025) on Artificial intelligence technologies in telecommunication development,⁸ this guide builds on the previously published [Guide Towards Collaborative AI Frameworks](#), extending its principles into a more practical framework for assessing preparedness and supporting implementation.

1.2 Why collaborative frameworks are becoming indispensable

AI frameworks need to be collaborative because AI technologies impact and intersect with multiple sectors and industries, requiring diverse expertise and joint action to ensure responsible development and deployment.⁹ The recent proliferation of AI-relevant laws has further reinforced this need. Several developments illustrate the reasons behind this trend. Under the European Union Artificial Intelligence Act (EU AI Act), a high-risk AI system used in credit scoring may simultaneously engage the banking supervisor, the data protection authority, consumer protection agencies and product-safety or market-surveillance authorities. No single authority can address all relevant aspects. In the United States, state laws governing automated decision-making systems must operate alongside federal enforcement by the Federal Trade Commission,¹⁰ the Equal Employment Opportunity Commission, the Consumer Financial Protection Bureau, sectoral regulators and general civil-rights law. In China, rules governing recommendation algorithms, deepfakes and generative AI involve cyberspace, content and security regulators, each with distinct mandates. In Africa and South Asia, the use of AI in agriculture, health or social protection is usually funded or technically supported by donors and international firms, adding layers of cross-border coordination on top of domestic oversight.

Collaborative AI frameworks provide structured ways to handle these complexities. They typically include a central coordination mechanism (for example, an AI council, AI office or interministerial committee); formal cooperation agreements between regulators (memoranda of understanding, joint guidance and joint enforcement protocols); multi-stakeholder advisory bodies, including civil society, academia and industry; and shared tools, such as common templates for AI impact assessment and model documentation, which reduce fragmentation and compliance burdens. Without such frameworks, authorities risk duplicating efforts, creating regulatory gaps, sending inconsistent messages to industry, and eroding public trust.

This is where the link between collaborative AI frameworks and AI preparedness becomes critical. A framework may identify the right institutions, coordination mechanisms and stakeholder channels, but it does not automatically ensure that those institutions have the authority, technical expertise, data access, infrastructure, procurement tools or enforcement capacity to govern AI in practice. Collaboration provides the governance model, while preparedness determines

⁸ International Telecommunication Union (ITU), World Telecommunication Development Conference 2025 (WTDC-25), Final Report, https://www.itu.int/dms_pub/itu-d/opb/tdc/D-TDC-WTDC-2025-PDF-E.pdf

⁹ International Telecommunication Union (ITU), AI for Good resources, <https://aiforgood.itu.int>

¹⁰ Federal Trade Commission (FTC) website, <https://www.ftc.gov>

whether that model can function effectively. This guide treats collaborative AI frameworks and AI preparedness diagnostics as mutually reinforcing: the framework clarifies which actors need to work together, while the diagnostic assesses whether they are ready to do so in a credible, proportionate and effective manner.

Linkages with ICT and digital infrastructure ecosystems

Collaborative AI frameworks do not operate in isolation but are deeply dependent on underlying ICT and telecommunication infrastructure, including connectivity, cloud and edge computing environments, data infrastructure and digital public infrastructure. Recognizing that traditional siloed regulation is no longer sufficient, the International Telecommunication Union (ITU) has advanced the concept of collaborative (G5) regulation,¹¹ emphasizing flexible, cross-sector and stakeholder-driven regulatory frameworks that can evolve alongside technological change.

As AI systems become more autonomous, opaque and scalable, regulation must be based on the collaborative foundations of G5, and incorporate concepts such as responsibility-by-design and continuous human oversight, including human-in-the-loop and human-on-the-loop approaches. Regulators should move from passive rule-setting to proactively building digital ecosystems, embedding ethical considerations throughout the technology lifecycle rather than relying only on reactive, post-deployment risk mitigation.

ITU research highlights that effective digital transformation depends on enabling regulatory frameworks, collaborative governance, robust digital infrastructure and coordinated policymaking that supports innovation while protecting consumers and promoting inclusive, sustainable growth. By fostering collaboration among governments, regulators, industry and civil society, G5 regulation helps to create resilient digital ecosystems that expand meaningful connectivity, bridge digital divides and maximize the social and economic benefits of digital technologies.

ICT regulators play a critical role within collaborative AI frameworks by enabling AI deployment, overseeing AI-enabled network management, ensuring secure and resilient infrastructure and supporting trusted data flows across sectors.

As highlighted throughout this guide, effective collaborative AI frameworks require alignment between AI policy instruments and preparedness in foundational digital infrastructure, particularly in broadband access, data ecosystems, cybersecurity and compute capacity.

1.3 Objectives and structure of this integrated guide

This updated and integrated guide is designed to help policy-makers and regulators turn AI policy goals into workable institutional and regulatory action. The preceding sections show that AI governance is no longer limited to high-level principles or isolated sectoral initiatives. It now requires coordinated action across digital ministries, ICT regulators, data protection authorities, cybersecurity bodies, competition and consumer agencies, sector regulators, procurement authorities, academia, industry and civil society. The guide, therefore, has two connected objectives. First, it updates and enriches the analysis of collaborative AI frameworks in the light of the latest legal, institutional and policy developments from 2023 to 2026. Second, it introduces a practical AI preparedness diagnostic to help national and subnational authorities

¹¹ ITU, G5 Accelerator, information on G5 Benchmark and digital readiness frameworks, <https://gen5.digital/>

assess whether the institutional, infrastructural, legal, technical and human-capacity foundations are in place to operationalize those collaborative frameworks.

The guide is structured in six main parts:

- Part 1 provides an introduction and situates collaborative AI frameworks in the current landscape.
- Part 2 presents a comprehensive update to reflect the latest approaches to collaborative AI frameworks, organized by region, highlighting their implications for collaborative frameworks.
- Part 3 introduces the concept, purpose and methodology of the AI preparedness diagnostic, including a detailed step-by-step approach combining document review, stakeholder interviews and institutional self-assessment.
- Part 4 sets out structured diagnostic components for each of the eight preparedness dimensions, with clear assessment questions, plain-language explanations and maturity levels.
- Part 5 brings the analysis together by showing how diagnostic findings can be synthesized and translated into phased roadmaps linked to available capacity.

2 Global overview of AI laws and regulations: Implications for collaborative frameworks (2023–2026)

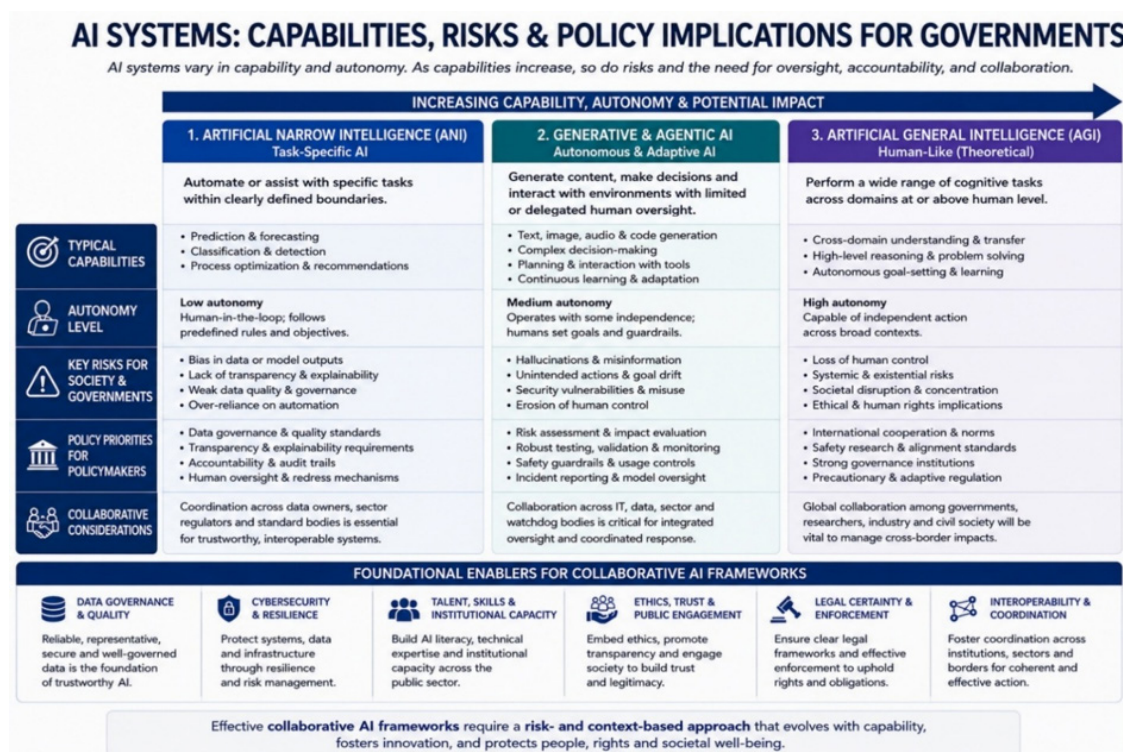
2.1 AI fundamentals: why they matter for preparedness

Artificial intelligence (AI) encompasses a diverse range of systems with varying capabilities and degrees of autonomy. At one end of the spectrum are **artificial narrow intelligence (ANI)** systems, designed to perform specific tasks such as prediction, classification and optimization. At the frontier are emerging concepts such as **artificial general intelligence (AGI)**, which could perform across domains with human-like flexibility; however, such systems currently remain largely theoretical. Between these two ends of the spectrum, recent advances have accelerated the development and deployment of **generative AI**, which produces text, images and code, and **agentic AI**, which can act autonomously, make decisions and interact with other systems to achieve defined goals.

Most AI systems today are powered by **machine learning (ML)**, which enables systems to learn patterns from data rather than follow explicit rules. Within ML, **unsupervised learning** is particularly relevant from a policy perspective, as it identifies patterns without predefined labels, making outcomes less predictable, less explainable and more difficult to audit.

These distinctions are not merely technical; they are essential for assessing **national AI preparedness**. Different types of AI create different levels of risk and therefore require different levels of institutional capacity, regulatory oversight and technical capability. For example, deploying ANI systems for routine public service optimization may require strong data governance, procurement practices and basic technical skills. In contrast, the use of generative or agentic AI introduces more complex challenges, including model transparency, misuse risks, cybersecurity vulnerabilities, and the need for continuous monitoring and human oversight. More advanced or hypothetical systems, such as AGI, raise systemic and cross-border considerations that may require anticipatory and internationally coordinated responses.

Figure 1: AI systems



Source: ITU

Understanding these differences allows policy-makers and regulators to move beyond generic approaches and design risk-based, proportionate and actionable collaborative AI frameworks. It enables countries to sequence their efforts, prioritize investments and align governance tools with the types of AI systems they are deploying or planning to deploy. In this regard, distinguishing among AI types is a critical first step in moving from high-level ambition to practical, implementable national AI preparedness strategies.

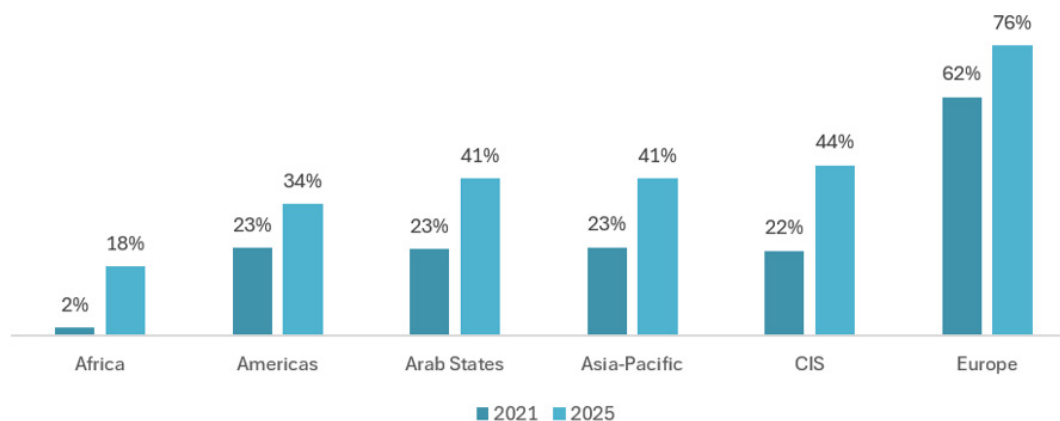
2.2 The evolution and diversity of AI regulatory approaches

Between 2023 and 2026, the global AI regulatory landscape shifted from principle-based guidance to legally binding instruments. However, this evolution has been uneven: while some jurisdictions have adopted comprehensive horizontal AI laws with detailed obligations and supervisory architectures, others continue to rely on existing sectoral and cross-cutting frameworks (data protection, telecoms, consumer and cyber frameworks) supplemented by AI strategies, ethics guidelines and pilot projects. Table 1 summarizes selected AI-specific laws and frameworks adopted or advanced during this period, organized by region.

The rapid expansion of national AI strategies and policies provides an important basis for understanding the next phase of AI governance. ITU data (Figure 2) show that between 2021 and 2025, the share of countries with AI strategies or policies increased across every region, albeit from very different starting points. Europe remains the most advanced region, rising from 62 per cent in 2021 to 76 per cent in 2025, while the Americas region, the Arab States region, the Asia and the Pacific region and the Commonwealth of Independent States (CIS) region all show significant growth. The Africa region also recorded progress, increasing from 2 per cent to 18 per cent over the same period. These findings confirm that AI policy adoption is no longer limited to early movers; it is becoming a global governance trend. At the same time, the regional

variation shown in the figure underlines why strategies alone are not sufficient. Countries now need to translate policy ambition into collaborative institutional arrangements, regulatory tools, infrastructure, skills and implementation capacity.

Figure 2: Artificial Intelligence strategies and policies, by region, 2021-2025



Source: ITU

Table 1: Comparative overview of regional AI collaborative frameworks and regulatory preparedness

Region	Dominant framework	What is driving convergence	What regulators should pay attention to	Preparedness questions for regulators
Americas	Mixed and multi-level. Canada is moving towards a federal high-impact AI regime; the United States relies on a layered federal-state-sectoral model; Latin America uses data protection laws and/or emerging AI-specific bills and strategies.	Growing interaction between privacy law, public-sector directives, sector regulators and state or provincial authorities.	Fragmentation across levels of government, overlap between privacy and AI oversight, and the need to align procurement, enforcement and sector supervision.	- Are mandates clear across federal, state/provincial, and sector bodies? - Are existing privacy and consumer laws enough, or are AI-specific rules needed? - Is there capacity to supervise high-impact use cases across sectors?

Table 1: Comparative overview of regional AI collaborative frameworks and regulatory preparedness (continued)

Region	Dominant framework	What is driving convergence	What regulators should pay attention to	Preparedness questions for regulators
Asia-Pacific	Hybrid; the region ranges from binding rules applicable to AI (China), to basic laws (focusing on promoting AI, as in Japan and the Republic of Korea), to more overarching digital-legislation-led approaches (India), to influential soft-law toolkits and testing frameworks (Singapore, Australia).	Use of laws, sector guidance, voluntary standards and testing tools to supplement or substitute for comprehensive AI legislation.	Whether soft law is actually influencing behaviour, how binding and non-binding tools interact, and whether regulators can oversee increasingly cross-sector deployments.	- Do voluntary frameworks produce measurable compliance? - Are sector regulators equipped to translate broad principles into enforceable practice? - Is coordination strong enough across digital, data protection and sector institutions?
Africa and Arab States	Foundational and developmental; AI governance is often built on data protection, digital transformation laws, national strategies, sector pilots and central coordination bodies, rather than horizontal AI statutes.	Expansion of digital ID, e-government, public-sector pilots, sandboxing and international partnerships are pushing countries towards more coordinated oversight.	Institutional maturity, basic data governance readiness, cybersecurity capacity, and whether ambitious AI deployment is moving faster than safeguards and supervisory capability.	- Are data protection and cybersecurity frameworks strong enough to support AI scaling? - Which institutions lead coordination? - Where are the biggest gaps: infrastructure, data governance, skills or sector oversight?

Table 1: Comparative overview of regional AI collaborative frameworks and regulatory preparedness (continued)

Region	Dominant framework	What is driving convergence	What regulators should pay attention to	Preparedness questions for regulators
Commonwealth of Independent States (CIS)	State-led and strategy-driven; governance is shaped more by central digital transformation agendas, presidential/cabinet strategies, sector rules and administrative coordination than by horizontal AI laws. Kazakhstan is moving towards a more structured AI law-based model, while Uzbekistan illustrates a strategy-led pathway.	Strong central state coordination, digital modernization goals, public-sector deployment and emerging regional cooperation through broader digital integration efforts.	Whether strategic ambition is matched by implementation capacity; how digital ministries, cybersecurity, data protection, sector ministries, and standards bodies work together; and whether public-sector deployment includes safeguards.	- Is there operational coordination beyond strategy documents? - Are data protection and cybersecurity frameworks sufficiently mature? - Do sector regulators have the expertise to supervise AI? - Are transparency, accountability and human oversight embedded in government deployment?

While these frameworks differ in legal force, scope and detail, they share common aspects that are directly relevant to collaborative frameworks:

- **Risk-proportionate obligations**, with high-risk AI systems (for example, those used in critical infrastructure, essential public or private services, law enforcement, justice, employment, credit scoring, education, health and border control) subject to enhanced scrutiny, transparency, human oversight and documentation requirements, while lower-risk and minimal-risk systems are subject to lighter or no specific obligations.
- **Value chain differentiation**, assigning distinct duties to providers (developers or producers of AI systems or general-purpose models), deployers (entities using AI systems in their operations or services), importers, distributors and other actors, which necessitates coordination among regulators to understand commercial arrangements, supply chains and outsourcing.
- **Increased attention to general-purpose AI and systemic risk**, particularly models with capabilities that could be used across many applications and that may pose systemic risks due to their reach, impact or potential misuse, triggering obligations on developers and requiring cooperation between digital, competition, data protection and sector regulators.
- **Stronger provisions on transparency, documentation and human oversight**, often including requirements for technical documentation, logging, explainability, human review of automated decisions, and in some cases public disclosure of the use of AI in decisions affecting individuals or communities.

- **Emphasis on multi-agency collaboration for implementation and enforcement**, reflected in provisions requiring national coordination bodies, joint guidance, information-sharing arrangements and cooperation on supervision and market surveillance.

These shared features explain why a regional review is necessary before introducing the diagnostic. The issue is not simply that countries are adopting different approaches to AI regulation; rather, each model gives rise to a different set of coordination, capacity and implementation challenges. A comprehensive AI act, a sector-led approach, a soft-law toolkit, a state-led digital transformation strategy or a data-protection-based model all require different institutional arrangements, capacities and different levels of preparedness. The following regional sections, therefore, show how collaborative AI governance is taking shape in practice and highlight the need for a diagnostic to move beyond legal comparison towards a practical assessment of countries ability to implement, supervise and sustain AI governance reforms.

2.3 European Union: The Artificial Intelligence Act (AI Act) and its collaborative AI requirements

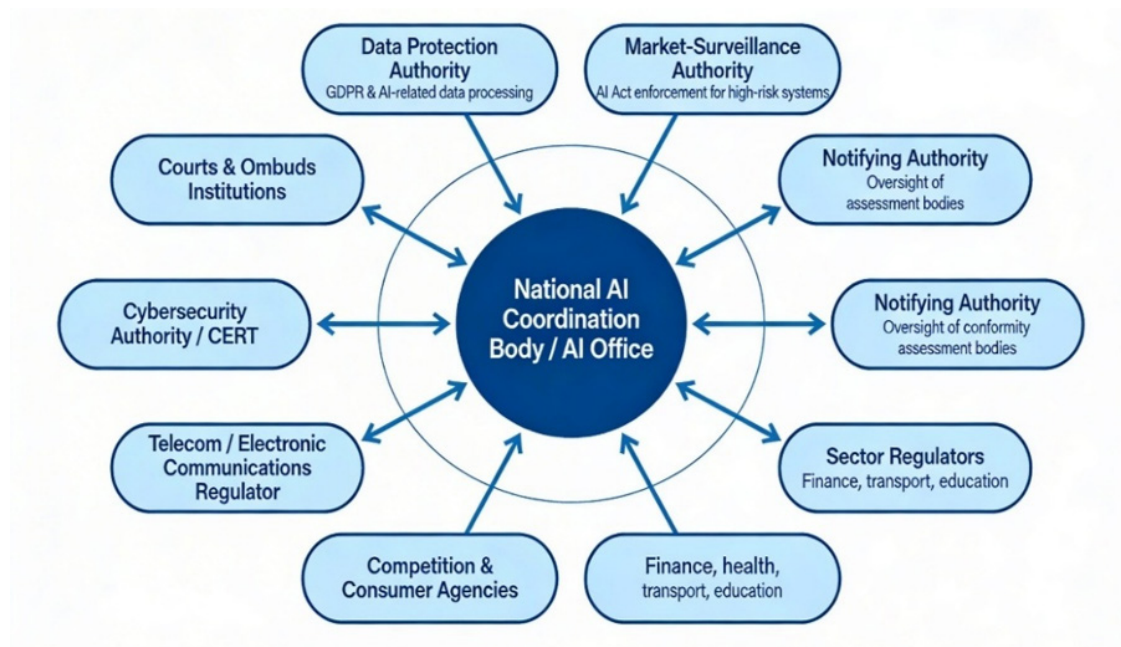
The European Union AI Act is one of the most comprehensive pieces of horizontal AI legislation.¹² Its core architecture can be understood along four main axes.

- **Scope:** The Act applies to providers placing AI systems on the European Union market and to deployers using AI systems in the European Union, regardless of their place of establishment, which gives the Act extraterritorial reach and creates a need for coordination with non-European Union jurisdictions.
- **Risk classification:** The Act establishes four categories of AI systems. **Unacceptable-risk systems** are prohibited, including certain manipulative systems, untargeted social scoring by public authorities and the use of real-time remote biometric identification in publicly accessible spaces for law enforcement, subject to narrowly defined exceptions. **High-risk systems** are subject to strict obligations on risk management, data governance, transparency, human oversight, accuracy, robustness and cybersecurity. **Limited-risk systems** are subject to transparency obligations including, for example, chatbots and emotion recognition systems. **Minimal-risk systems** are largely exempt from mandatory requirements.
- **Obligations across the AI value chain:** Providers of high-risk systems must establish and maintain risk management systems, ensure data quality, maintain comprehensive technical documentation, enable logging, provide information to deployers, ensure human oversight and meet requirements relating to robustness and cybersecurity. Deployers must use systems appropriately, monitor operations and, in some cases, conduct fundamental-rights impact assessments.
- **Governance and supervision:** Member States should designate notifying authorities for conformity assessment bodies, market-surveillance authorities responsible for enforcement of the EU AI Act, and authorities responsible for protecting fundamental rights where relevant. They must also participate in the work of a European Artificial Intelligence Board and coordinate with the European AI Office, which oversees implementation, particularly for general-purpose AI models with systemic risk.
- **The Digital Omnibus:** In November 2025, the European Commission adopted the Digital Omnibus package, made up of two proposed regulations: one on data, cybersecurity and privacy rules, and one on AI Act implementation, known as the AI Omnibus. Its aim is to simplify the European Union digital rulebook, reduce compliance costs and legal uncertainty, while preserving the core objectives of European Union digital regulation. The

¹² European Commission, AI Act, regulatory framework for artificial intelligence, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

Digital Omnibus proposes a single-entry point mechanism for cybersecurity incident and data breach reporting, restructuring parts of European Union data legislation into the Data Act, and repealing the Platform-to-Business Regulation where it overlaps with the Digital Services Act.¹³ The AI Omnibus introduces targeted amendments to the AI Act: aligning high-risk AI obligations with the availability of standards and support tools, extending simplifications to SMEs and small mid-caps, strengthening the AI Office oversight role, and expanding real-world testing and sandbox flexibility. A political agreement on the AI Omnibus was reached on 7 May 2026. One key outcome is an extended transition period until 2 August 2028 for certain high-risk AI systems embedded in regulated products. It should be noted that the Omnibus package is not a rollback of the AI Act, but rather an implementation and simplification package. The European Union is trying to make its digital and AI rules more workable, proportionate and innovation-friendly, while keeping the risk-based regulatory model in place.¹⁴

Figure 3: Illustrative AI collaborative framework architecture in a European Union Member State under the AI Act



Source: ITU

A preparedness diagnostic in a European Union Member State should consider how well these bodies are resourced, how they coordinate (through formal councils, joint working groups, memoranda of understanding or ad hoc contacts), whether they have AI-specific expertise and tools (such as algorithmic audit methods, access to technical experts, cooperation with academia and civil society), and whether clear procedures exist for assigning responsibilities

¹³ European Commission, Digital Omnibus Regulation Proposal, Library, 2025, <https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal>

¹⁴ White & Case, "EU agrees Digital Omnibus deal to simplify AI rules", Insights, 2006, <https://www.whitecase.com/insight-alert/eu-agrees-digital-omnibus-deal-simplify-ai-rules>

and escalating issues. Countries such as Spain¹⁵ and Germany¹⁶ have already begun assessing and organizing the institutional, supervisory, and technical arrangements needed for AI Act implementation, including the designation of competent authorities, guidance for high-risk AI systems, market surveillance structures, single points of contact, regulatory sandboxes and coordination with sectoral regulators.

2.4 Americas: diverse regulatory models and emerging convergence

In the Americas region, AI governance reflects different constitutional and market structures; however, common themes of multi-level and multi-agency collaboration are emerging.

Canada has advanced the Artificial Intelligence and Data Act (AIDA), as part of Bill C-27, which would regulate "high-impact" AI systems under federal jurisdiction.¹⁷ This directive serves as a practical model for public-sector AI governance and demonstrates how a central policy instrument can drive coordination across departments and agencies. A preparedness diagnostic in Canada would examine the interface between AIDA, existing privacy law (Personal Information Protection and Electronic Documents Act (PIPEDA) or its successor), the above-mentioned directive, sectoral regulators (such as the Office of the Superintendent of Financial Institutions, the Canadian Radio-television and Telecommunications Commission) and provincial authorities, which retain significant powers over areas such as health, education and social services.

In the **United States**, AI governance continues to reflect a federated, multi-level system characterized by significant diversity and complexity. However, the federal policy baseline shifted materially in 2025. Rather than moving towards a single horizontal AI statute, the United States has continued to rely on a layered model in which executive action, voluntary technical frameworks, sector-specific oversight and state legislation all play important roles. At the federal level, Executive Order 14179, issued on January 23, 2025, redirected United States AI policy towards removing barriers to American leadership in artificial intelligence and revoked the prior Biden-era executive framework. This policy direction was subsequently operationalized through two Office of Management and Budget (OMB) memoranda, both issued in April 2025: M-25-21 on accelerating federal use of AI through innovation, governance, and public trust, and M-25-22 on efficient acquisition of AI in government. In July 2025, the White House issued Winning the AI Race: America's AI Action Plan, setting out more than 90 federal actions across innovation, infrastructure and international diplomacy and security. The policy trajectory was further reinforced by the Executive Order of 2 June 2026, "Promoting Advanced Artificial Intelligence Innovation and Security", which introduced a voluntary framework for federal

¹⁵ For further information on Spain's AI Act implementation, see the website of the Government of Spain, <https://www.lamoncloa.gob.es/consejodeministros/referencias/paginas/2025/20250311-referencia-rueda-de-prensa-ministros.aspx>; resources on practical compliance guides are available on the Spanish Agency for the Supervision of Artificial Intelligence (AESIA), <https://aesia.digital.gob.es/en/present/resources/practical-guides-for-ai-act-compliance> and the Government website, <https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/transformacion-digital-y-funcion-publica/paginas/2025/111225-lopez-empresas-guias-ia.aspx>. Information relating to the 2024 Artificial Intelligence Strategy is available at https://digital.gob.es/content/dam/portal-mtdfp/DigitalizacionIA/1_DOSSIER_AI_ENGLISH_15_JULIO.pdf.

¹⁶ Further information on implementation of EU AI Act obligations is available on the websites of the Federal Government, <https://www.bundesregierung.de/breg-de/aktuelles/umsetzung-ki-verordnung-2406638>, and of the Bundestag, <https://www.bundestag.de/dokumente/textarchiv/2026/kw12-de-kuenstliche-intelligenz-1151800>. Additional resources on governance, including the single point of contact, competent authorities under Article 70 of the AI Act and market surveillance, are available on the site of the Bundesnetzagentur, https://www.bundesnetzagentur.de/EN/Areas/Digitalisation/AI/11_Governance/start.html.

¹⁷ Parliament of Canada. Bill C-27, Digital Charter Implementation Act, 2022, first reading, <https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading>

review of covered frontier models, including pre-release access for up to 30 days to assess advanced cyber capabilities, while explicitly avoiding mandatory licensing or preclearance requirements. Taken together, these measures indicate that current United States federal AI policy is oriented less towards broad horizontal risk regulation and more towards accelerated adoption, procurement reform, infrastructure build-out, voluntary security cooperation with industry and national competitiveness.¹⁸

This shift has not diminished the importance of technical governance tools and sector-specific enforcement. The National Institute of Standards and Technology AI Risk Management Framework provides voluntary guidance widely used across government and industry.¹⁹ Sectoral agencies, such as the Federal Trade Commission (consumer protection and competition)²⁰, the Consumer Financial Protection Bureau (financial services),²¹ the Equal Employment Opportunity Commission (employment discrimination)²², the Food and Drug Administration (medical devices and digital health) and the Department of Health and Human Services (health AI)²³ issue guidance, undertake enforcement action and, in some cases, adopt rules governing AI-related practices. At the state level, numerous AI laws have been enacted, increasing the need for coordination between federal and state regulators and among sectoral agencies within states, especially where AI services operate across jurisdictions. Experience from state-level preparedness initiatives, including the AI Readiness Project, supported by organizations such as New America, has also informed the development of sectoral AI action plans and procurement reforms.²⁴

In **Latin America and the Caribbean**, AI governance is integrating emerging AI-specific instruments into existing data protection and consumer frameworks with. Brazil has advanced Bill 2338/2023, a comprehensive piece of AI draft legislation influenced by the EU AI Act, which proposes risk-based obligations for AI providers and deployers and foresees the creation of an AI authority that would work closely with the National Data Protection Authority²⁵ and sectoral regulators, including the Central Bank of Brazil, the health regulator (Agência Nacional de Saúde Suplementar / National Supplementary Health Agency of Brazil) and the telecommunications regulator ANATEL. Data protection laws modelled on the GDPR or reflecting broader regional convergence, such as the Federal Law on Protection of Personal Data in Mexico, the data protection law in Chile, the Personal Data Protection Act in Argentina, already apply to AI-related processing. Data protection authorities increasingly interpreting and enforcing them

¹⁸ See information on AI on the United States Government website <https://www.ai.gov/>

¹⁹ National Institute of Standards and Technology (NIST), Artificial Intelligence Risk Management Framework, <https://www.nist.gov/itl/ai-risk-management-framework>

²⁰ See the website of the Federal Trade Commission (FTC), <https://www.ftc.gov/>; including resources on AI, <https://www.ftc.gov/industry/technology/artificial-intelligence>.

²¹ See the website of the Consumer Financial Protection Bureau (CFPB), <https://www.consumerfinance.gov/>, including resources on AI, <https://www.consumerfinance.gov/ai/>.

²² See the website of the Equal Employment Opportunity Commission (EEOC), <https://www.eeoc.gov/>, including resources on AI and the Americans with Disabilities Act, <https://www.eeoc.gov/eeoc-disability-related-resources/artificial-intelligence-and-ada>.

²³ See the website of the United States Department of Health and Human Services (HHS); <https://www.hhs.gov/>; including resources on AI, <https://www.hhs.gov/programs/topic-sites/ai/index.html>.

²⁴ Colorado adopted the Artificial Intelligence Act in 2024, addressing algorithmic discrimination in consumer-facing consequential decisions such as credit, employment, housing and insurance, and assigning enforcement to the state Attorney General. California has passed legislation on automated decision systems, algorithmic transparency, deepfakes, and is considering additional proposals on frontier AI models and public-sector AI. States including New York, Illinois, Connecticut, Tennessee, and Virginia have introduced laws or rules on AI in employment, credit scoring, biometrics, and consumer protection, often focusing on bias, transparency, and notice obligations. See: <https://www.newamerica.org>.

²⁵ Government of Brazil, Lei Geral de Proteção de Dados Pessoais (LGPD), enforced by the Autoridade Nacional de Proteção de Dados (ANPD), http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

in the context of AI. National AI strategies and ethics guidelines in countries including Chile, Uruguay and Colombia also signal interest in more structured governance, often linked to digital transformation programmes supported by the Inter-American Development Bank, the World Bank and United Nations agencies. Collaborative AI frameworks in the region often bring together digital ministries, data protection authorities, telecommunications regulators and sector regulators to address cross-cutting issues. A preparedness diagnostic can help to identify capacity and coordination gaps and inform the sequencing of governance reforms.

2.5 Asia-Pacific: hybrid approaches from binding rules to soft-law toolkits

Regulatory approaches in the Asia and Pacific region range from prescriptive, binding rules to framework laws and influential soft-law instruments.

China has adopted several binding measures that apply directly to AI governance. The Regulation on the Administration of Algorithmic Recommendation Services (in force as of 2022) requires providers – including social media platforms, e-commerce sites and content aggregators – to file algorithmic recommendation services with authorities, to ensure transparency and user control, and to implement security and content moderation measures.²⁶ The Provisions on the Administration of Deep Synthesis Internet Information Services target deepfake and synthetic media technologies, establishing obligations for labelling AI-generated content, ensuring authenticity of information, conducting security assessments and filing services with authorities. The Interim Measures for the Management of Generative AI Services (2023) apply to generative AI providers, requiring them to ensure content accuracy and alignment with "core socialist values," conduct security assessments and register certain services, and manage training data use to prevent illegal or harmful outputs. These measures, which involve multiple authorities, including the Cyberspace Administration, content and security regulators, illustrate how AI governance is embedded in a broader content, security and digital policy framework that emphasizes state oversight and social stability.

In **Japan**, the government has enacted the Act on the Promotion of Research, Development and Utilization of AI-related Technologies (AI Promotion Act), which provides a "basic law" framing AI policy.²⁷ The Act seeks to promote AI research and development and deployment across sectors, ensure that AI use respects safety, human rights and societal values, and facilitate cooperation among government, industry and academia. A subsequent Basic Plan for Artificial Intelligence outlines specific initiatives and institutional arrangements. The Government of Japan approach relies heavily on sectoral regulators, voluntary guidelines and co-regulation, supported by the AI Promotion Act as a coordination anchor, and uses a model in which a framework law sets out principles and government responsibilities, while detailed obligations are developed at the sectoral level and through soft law.

In the **Republic of Korea**, the AI Basic Act sets out principles, government support measures and references to ethics and safety, underpinning policies such as the Korea New Deal and AI-driven

²⁶ Cyberspace Administration of China (CAC), Announcements and regulatory materials on algorithmic recommendation, deep synthesis, and generative AI services, <http://www.cac.gov.cn>.

²⁷ For information on Japan's national AI strategy and analysis of the AI Promotion Act, see the website of the Government of Japan at https://www.cas.go.jp/jp/seisaku/ai_senryaku/index.html or Future of Privacy Forum, <https://fpf.org/blog/understanding-japans-ai-promotion-act-an-innovation-first-blueprint-for-ai-regulation/>.

industrial strategies.²⁸ It relies on existing sector regulators, data protection authorities and digital ministries to enforce AI-related obligations. In this context, a preparedness diagnostic would assess coordination mechanisms, sector-specific capacities and the interaction between soft-law and hard-law instruments.

The Government of **India** is developing AI governance primarily through broader digital legislation and sectoral initiatives. A forthcoming Digital India Act is expected to address AI alongside platforms and data governance, while the Digital Personal Data Protection Act (DPDP) provides a basis for regulating AI-driven data processing.²⁹ Sector regulators such as the Reserve Bank of India³⁰ and the Securities and Exchange Board of India use regulatory sandboxes and guidelines to supervise AI-based financial products and services. National AI strategy documents and initiatives such as "AI for All" combine innovation promotion with references to ethics, trust and inclusion. A preparedness diagnostic in India would need to map the interaction between DPDP enforcement, emerging digital platform rules, sectoral AI initiatives and the role of the federal versus state authorities in areas like health and education.

Singapore has become a reference for non-binding but influential AI governance tools. The Personal Data Protection Commission (PDPC) has issued two editions of the Model AI Governance Framework, which focuses on transparency, fairness, human oversight and accountability, providing practical guidance for firms and government agencies.³¹ AI Verify, launched by PDPC and the Infocomm Media Development Authority, is an open-source testing framework that enables organizations to assess AI systems against governance criteria such as explainability, fairness and robustness.³² Enforcement relies largely on PDPC under the Personal Data Protection Act, the Monetary Authority of Singapore (MAS)³³ for financial services, and sectoral regulators using existing laws, supplemented by voluntary compliance with the Model Framework and use of AI Verify. This model illustrates how soft-law and testing tools can drive governance practice and support regulatory oversight, even in the absence of AI-specific binding legislation.

At the regional level, ASEAN is also moving towards a network-based model of AI safety cooperation. ASEAN AI SAFE offers a practical example of regional collaborative AI governance. Established by ASEAN Member States in October 2025, the network is designed to help countries unlock AI benefits while managing its risks through cooperation, capacity-building, research, best-practice exchange and partnerships. It shows how countries with different levels of AI maturity can pool expertise, strengthen AI safety capabilities and align safeguards for cross-border risks without requiring every country to build the same institutions at the same pace.³⁴

²⁸ For information on AI initiatives and policy resources, see the website of the Ministry of Science and ICT of the Republic of Korea, at <https://www.msit.go.kr>; see also the website of the Center for Security and Emerging Technology within Georgetown University Walsh School of Foreign Service, <https://cset.georgetown.edu/publication/south-korea-ai-law-2025/>.

²⁹ For information on AI and Digital India policy initiatives of the Government of India, see the website of the Ministry of Electronics and Information Technology (MeitY), <https://www.meity.gov.in>; see also the IndiaAI knowledge portal, <https://indiaai.gov.in/>.

³⁰ Reserve Bank of India, <https://www.rbi.org.in>.

³¹ Singapore Personal Data Protection Commission (PDPC), "Singapore's Approach to AI Governance", Model AI Governance Framework, <https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework>.

³² AI Verify Foundation / Singapore, AI Verify testing framework, <https://aiverifyfoundation.sg/what-is-ai-verify/>.

³³ Monetary Authority of Singapore (MAS), <https://www.mas.gov.sg>.

³⁴ Association of Southeast Asian Nations (ASEAN), Declaration on the Establishment of an ASEAN AI Safety Network (ASEAN AI SAFE), <https://asean.org/declaration-on-the-establishment-of-an-asean-ai-safety-network-asean-ai-safe/>.

In **Australia**, responsible AI principles for government have been developed, consultations have been held on AI regulation options and a voluntary AI Safety Standard has been introduced, aligned with international guidelines.³⁵ Regulators such as the Australian Competition and Consumer Commission (ACCC)³⁶ and the Office of the Australian Information Commissioner (OAIC)³⁷ are exploring AI-specific guidance under their existing mandates. A preparedness diagnostic would assess the coordination among these bodies, the effectiveness of voluntary standards and the extent to which sectoral regulation addresses AI risks.

2.6 Africa and Arab States: building from data and digital foundations

In many African countries, AI governance begins with data protection and digital transformation laws and policies, complemented by AI strategies and sectoral pilots.

South Africa has the Protection of Personal Information Act, enforced by the Information Regulator.³⁸ AI is governed primarily through this framework, supplemented by sectoral regulators (for example, the Health Professions Council, financial regulators) and digital transformation initiatives led by the Department of Communications and Digital Technologies. A national AI strategy is under development to align these efforts. In **Nigeria**, the Nigeria Data Protection Regulation and the Nigeria Data Protection Commission, along with guidelines from the National Information Technology Development Agency³⁹ and a national AI policy, steer AI use in both public and private sectors. Sectoral guidelines from the Central Bank of Nigeria and other regulators address AI in finance and other domains. In **Kenya**, the government is updating ICT and data governance frameworks and launching AI pilots in agriculture and public services, in coordination with the Communications Authority of Kenya,⁴⁰ the Office of the Data Protection Commissioner and sectoral ministries. **Rwanda** has a National AI Policy that positions AI as a tool for development in agriculture, health and public administration, assigning responsibilities to the Ministry of ICT and Innovation, the Rwanda Information Society Authority and sector ministries.⁴¹

In the **Arab States** region, the Government of the **United Arab Emirates** has appointed a Minister of State for Artificial Intelligence and developed comprehensive strategies and guidelines that work through entities such as Smart Dubai⁴² and sectoral regulators, positioning AI as central to economic diversification and public-sector transformation. A Federal Artificial Intelligence and Data Authority has also been established to act as the single national body responsible for data, artificial intelligence and digital government, to be chaired by the Minister of State

³⁵ For information on AI policy resources of the Government of Australia (Department of Industry, Science and Resources), see <https://www.industry.gov.au/science-technology-and-innovation/technology/artificial-intelligence>.

³⁶ For information on the Australian Competition and Consumer Commission (ACCC), see <https://www.accc.gov.au>, and also <https://www.accc.gov.au/about-us/accc-role-and-structure/governance-and-accountability/artificial-intelligence-ai-transparency-statement>.

³⁷ For information on the Office of the Australian Information Commissioner (OAIC), see <https://www.oaic.gov.au>, including the AI transparency statement at <https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/oaic-ai-transparency-statement>.

³⁸ South Africa Information Regulator, <https://www.justice.gov.za/infoereg/>.

³⁹ Nigeria National Information Technology Development Agency (NITDA), <https://nitda.gov.ng>.

⁴⁰ Communications Authority of Kenya, <https://www.ca.go.ke>; also see the section of the regulator website on its regulatory sandbox <https://www.ca.go.ke/regulatory-sandbox> and responsible use of AI <https://www.ca.go.ke/authority-calls-responsible-use-artificial-intelligence-world-marks-safer-internet-day>.

⁴¹ For further information, see the website of the Rwanda Ministry of ICT and Innovation, <https://www.minict.gov.rw>, including its AI policy, <https://www.minict.gov.rw/ai-policy>.

⁴² Smart Dubai, <https://www.smartdubai.ae>.

for AI.⁴³ In **Saudi Arabia**, the Saudi Data and AI Authority (SDAIA)⁴⁴ coordinates data and AI policy, supervises implementation of the national data strategy and supports AI adoption in Vision 2030 programmes, working with line ministries and regulators. In **Jordan**, the government has adopted a strategic, coordination-led approach, through its national AI policy and implementation roadmap, led by the Ministry of Digital Economy and Entrepreneurship and supported by cross-government digital transformation institutions.⁴⁵ These institutional arrangements highlight the role of central AI bodies in environments where comprehensive AI legislation is absent but strategic direction and coordination are crucial.

Collaborative AI frameworks in Africa and the Arab States often rely on coordination between data protection authorities, digital ministries, telecommunications regulators, cybersecurity agencies and sector regulators. Horizontal and binding AI-specific laws remain less common in the region as of early 2026, but public-sector pilots, sandbox regimes and international partnerships (for example with the African Union Continental AI strategy, the Smart Africa Alliance, United Nations agencies and development banks) are multiplying, which makes preparedness diagnostics particularly relevant for identifying where to invest in infrastructure, data governance, skills and institutional coordination before scaling high-risk AI deployments.

2.7 Commonwealth of Independent States: state-led digital transformation, strategic coordination and uneven regulatory maturation

Across the Commonwealth of Independent States (CIS), AI governance is evolving through a state-led model in which digital transformation agendas, national technology strategies, data governance rules and sectoral regulation play a more prominent role than comprehensive horizontal AI laws. As in other regions, collaborative AI frameworks are becoming necessary as AI deployment increasingly cuts across telecommunications, public administration, finance, education, health and security. However, in the context of the CIS region, coordination is often carried out by central executive institutions, digital ministries and presidential or cabinet-level strategies rather than solely by independent cross-sector regulators. A preparedness diagnostic in the region would therefore assess not only whether AI-specific rules exist, but also how responsibilities are distributed among digital development ministries, data protection and cybersecurity authorities, sector ministries and national standard-setting bodies. The overall approach in the CIS region would therefore differ from those in other regions.

Kazakhstan appears to be moving furthest towards a dedicated AI governance framework in this region. Recent government reporting indicates that the government has adopted a standalone Artificial Intelligence Law and is embedding it within a broader institutional ecosystem that includes a national AI platform, sovereign computing infrastructure, public-sector deployment measures and support for Kazakh-language models. This points to a more structured governance architecture in which legal obligations, infrastructure planning, industrial policy and human capital development are being developed in parallel. A preparedness diagnostic would therefore assess not only the new legislation, but also its interaction with personal data

⁴³ Paul, Ajanta. "Sheikh Mohammed announces formation of UAE's AI and data authority." Khaleej Times, 14 June 2026, updated 14 June 2026, <https://www.khaleejtimes.com/uae/uae-authority-ai-data-digital-government>.

⁴⁴ Saudi Data and AI Authority (SDAIA), <https://sdaia.gov.sa/en>.

⁴⁵ See the artificial intelligence policy page of the Jordan Ministry of Digital Economy and Entrepreneurship, <https://modee.gov.jo/en/pages/aicustompage>

protection, information security, consumer protection, sectoral supervision and implementation capacity across ministries and local authorities.⁴⁶

The approach adopted in **Uzbekistan** reflects another important pathway: governance through a national AI strategy linked to broader digital transformation and state-capacity goals. The national Strategy for the Development of Artificial Intelligence Technologies until 2030, approved in October 2024, sets measurable targets, includes an implementation plan for 2024–2026 and links AI development to infrastructure, public-sector modernization, big data and workforce development. This is significant because it shows how some countries in the CIS region are building AI governance outward from development planning and administrative reform, rather than beginning with a risk-based statute. In such contexts, a collaborative AI framework is especially useful for clarifying institutional mandates, sequencing reforms and ensuring that data governance, procurement rules, public-sector ethics and sectoral oversight mature in parallel with deployment ambitions.⁴⁷

At the regional level, coordination remains more limited than in the European Union, but signs of convergence are emerging through broader digital cooperation mechanisms. The Eurasian Economic Union continues to advance its digital agenda and has begun to consider the role of AI in areas such as statistics, economic processes and digital integration. These developments do not yet amount to a binding, supranational AI regime. Instead, they point to an emerging regional layer in which interoperability, standards, compute access and public-sector use cases may gradually shape governance practices across parts of the CIS region. For the preparedness diagnostic, this means assessing regional institutional alignment, standards cooperation and cross-border digital market objectives alongside national legal and institutional readiness.⁴⁸

Overall, examples from the CIS region demonstrate that AI readiness and preparedness cannot be assessed solely by whether a country has adopted an AI act. In many jurisdictions in the CIS region, more relevant questions are whether central strategic direction is matched by operational coordination, whether sectoral institutions have the expertise to supervise AI use in practice, whether data protection and cybersecurity frameworks are sufficiently mature, and whether safeguards for transparency, accountability and human oversight accompany public-sector deployment. A collaborative AI framework can therefore serve as a practical bridge between state-led innovation ambitions and the institutional capacities needed to manage cross-cutting risks.

2.8 Cross-cutting trends and their implications for collaborative governance

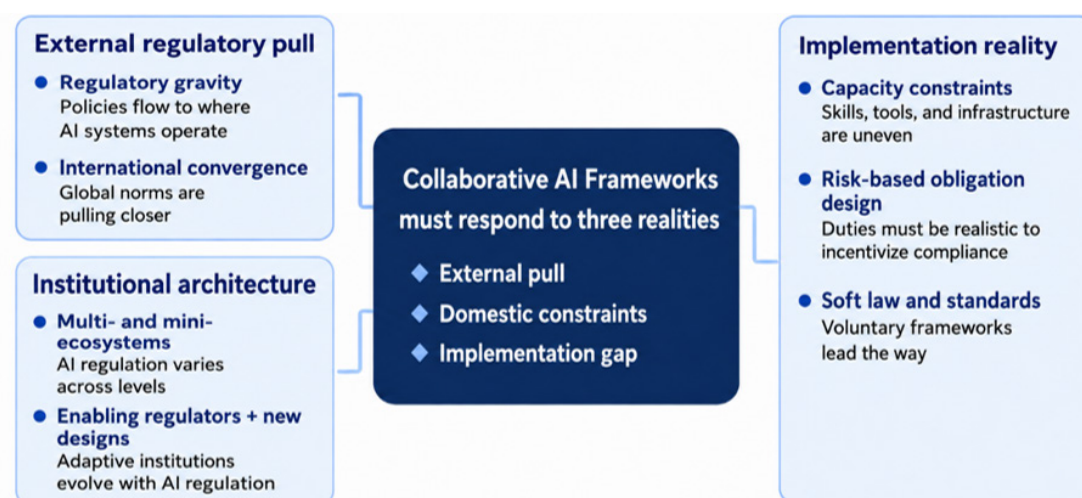
Across all regions, several structural features of the emerging AI regulatory environment have direct implications for the design and operation of collaborative frameworks.

⁴⁶ Government of Kazakhstan, Press release on artificial intelligence law and related national AI initiatives, <https://www.gov.kz/memleket/entities/maidd/press/news/1>.

⁴⁷ Information on Uzbekistan's AI development strategy, progress toward becoming a regional IT hub, and planned AI specialist training through 2030 can be found on the website of the Government of Uzbekistan, available at <https://lex.uz/en/docs/7159258>, as well as in *Oxford Insights*, available at <https://oxfordinsights.com/insights/harnessing-ai-for-development-uzbekistans-progress-towards-becoming-a-regional-it-hub>, and *Euronews*, available at <https://www.euronews.com/2025/11/28/uzbekistan-to-dramatically-reduce-bureaucracy-and-train-5-million-ai-specialists-by-2030>.

⁴⁸ Eurasian Economic Commission, Roadmap for the development of economic processes within the EAEU for five years, <https://eec.eaeunion.org/en/news/utverzhdena-dorozhnaya-karta-po-razvitiyu-ekonomicheskikh-protsessov-v-ramkakh-eaes-na-pyat-let>

Figure 4: Seven features shaping the AI regulatory landscape



Source: ITU

- **Regulatory gravity and alignment pressures.** Frameworks such as the EU AI Act, federal and state approaches in the United States, and the Government of China AI rules shape global expectations, supply chains and business practices. Smaller jurisdictions and those with close trade or data flows to these regions face de facto pressure to align, hybridize or explain divergence. These pressures come from trade relationships, reputational considerations and the need to ensure technical interoperability. A preparedness diagnostic should therefore not only assess whether appropriate "laws and institutions" exist but also how they "relate to dominant external frameworks", and whether competent authorities have the capacity to "manage divergences or mutual recognition arrangements".
- **Multi-regulator ecosystems.** AI law intersects with a wide range of regulatory domains, including data protection (such as GDPR, LGPD, POPIA, DPDP), telecommunications and electronic communications (including spectrum management, network management and platforms), consumer protection (including unfair practices and dark patterns), competition (including algorithmic collusion and abuses of dominance by AI platform providers), cybersecurity (including AI system security and adversarial attacks) and sectoral regulation (including finance, health, transport, education and social protection). Implementation depends on the capacity of relevant agencies – such as the European Data Protection Board,⁴⁹ national data protection authorities (DPAs), telecommunications regulators such as ARCEP⁵⁰ in France or ANATEL in Brazil,⁵¹ competition authorities such as the United Kingdom Competition and Markets Authority,⁵² AI councils in the United Arab Emirates and Saudi Arabia, and sector-specific regulators, to ensure effective coordination through councils, working groups, joint guidance and shared supervisory tools.
- **Capacity asymmetries.** Many low-income countries face deficits in infrastructure, data governance and skills deficits, even as the potential benefits of AI in agriculture, health and education are compelling. Legal transplants without corresponding capacity investments can result in unenforceable rules, implementation gaps and loss of public trust. A preparedness diagnostic can identify these gaps early and help to sequence reforms so that legal frameworks, institutions and capacity develop in parallel, rather than legislation advancing faster than implementation capacity.

⁴⁹ European Data Protection Board (EDPB), <https://edpb.europa.eu>.

⁵⁰ For further information, see the website of the French Electronic Communications, Postal and Print Media Distribution Regulatory Authority (ARCEP), <https://en.arcep.fr/arcep.html>.

⁵¹ See website of the Brazil National Telecommunications Agency (ANATEL - Agência Nacional de Telecomunicações), <https://www.gov.br/anatel/pt-br>.

⁵² See the website of the United Kingdom Competition and Markets Authority (CMA), <https://www.gov.uk/government/organisations/competition-and-markets-authority>.

- **Shift from principles to enforceable obligations and risk-based focus.** Many countries are moving from non-binding ethics principles towards binding obligations, especially for high-risk AI systems for example biometric identification, essential services, law enforcement, employment and credit. These frameworks often establish explicit duties for providers, deployers and other actors across the AI value chain. This shift places greater demands on regulators to understand the technical and commercial aspects of AI, conduct algorithmic audits, interpret documentation and logs, and coordinate across legal regimes.
- **Use of existing regulators, supported by new coordination bodies.** Rather than creating a single "AI regulator", most frameworks rely on existing competent authorities, including data protection, telecommunications, competition, consumer and sector-specific regulators – supported by new coordination bodies or AI offices (for example, the European Union AI Office,⁵³ national AI councils and inter-ministerial committees). This approach strengthens the need for collaborative frameworks and makes preparedness diagnostics particularly important for understanding whether coordination mechanisms are fit for purpose.
- **Soft law and voluntary standards where binding law lags.** In jurisdictions without horizontal AI laws, regulators use soft law (guidelines, frameworks, voluntary codes of practice such as the Model Framework in Singapore and the AI Safety Standard in Australia) and adapt existing sectoral mandates to AI, often referencing international standards such as International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) standards on AI, the OECD AI Principles⁵⁴ and the United Nations Educational, Scientific and Cultural Organization (UNESCO) Recommendation on the Ethics of Artificial Intelligence.⁵⁵
- **International convergence and the "Brussels effect".** Instruments such as the OECD AI Principles, the UNESCO Recommendation, the Council of Europe AI Convention and the EU AI Act exert a "Brussels effect" and normative pull, leading countries such as Brazil and Canada to develop frameworks with similar scopes, concepts and risk categorizations. At the same time, divergences – for example, between the European Union rights-based approach, the Government of China content and security focus, and the sectoral and innovation-oriented model in the United States – create additional complexity for multinational AI providers and highlight the need for mechanisms to support interoperability and mutual recognition.

These trends reinforce the central thesis of the guide: AI oversight and implementation cannot be achieved through laws, strategies or ethical principles alone. As AI systems are deployed in areas such as credit, health, education, public administration, law enforcement, telecommunications and other high-impact domains, countries need collaborative frameworks that connect the relevant institutions and preparedness diagnostics that assess whether those institutions have the capacity to perform their roles effectively. The diagnostic should not be treated as a separate exercise. It helps to translate international regulatory developments into concrete national priorities, institutional roles and implementation steps: it can help policy-makers to identify unclear mandates, weak infrastructure, fragmented data systems, skills gaps, outdated procurement rules and oversight tools in need of strengthening before AI is deployed at scale.

⁵³ European Commission, European AI Office, <https://digital-strategy.ec.europa.eu/en/policies/ai-office>.

⁵⁴ OECD AI Principles overview, <https://oecd.ai/en/ai-principles>.

⁵⁵ UNESCO, Recommendation on the Ethics of Artificial Intelligence, <https://unesdoc.unesco.org/ark:/48223/pf0000381137>.

3 Concept, purpose and methodology of a practical AI preparedness diagnostic

3.1 What is AI preparedness for policy-makers and regulators, and why does it matter?

"AI preparedness" is often discussed in high-level comparative terms, including rankings on global indices, traffic-light dashboards, and the classification of countries as "leaders," "followers" or "laggards." While such benchmarks can help to situate countries in the global landscape, they are not primarily designed to address the practical tasks of regulators and policy-makers: drafting legislation, supervising high-risk systems, coordinating across ministries and agencies, procuring AI tools for public use, and determining when and how to deploy AI in areas such as social protection, health, finance, policing and telecommunications. A practical AI preparedness diagnostic must address a more concrete question: given a country's existing policies, institutions, infrastructure, data governance practices, skills, innovation environment, ethics frameworks and enforcement capacity, which AI-related actions are feasible, in what sequence, and subject to which safeguards?

AI preparedness diagnostics are most useful when they help governments to make concrete choices about priorities, sequencing, capacity-building and safeguards. For policy-makers and regulators, the real value is not simply knowing whether a country ranks high or low on a global index, but understanding what can be done next, by whom, in what sequence, and with what safeguards. These tools help countries to identify whether their institutions have clear mandates, whether regulators can coordinate across sectors, whether data systems and digital infrastructure are strong enough to support AI deployment, whether public officials have the skills to procure and oversee AI responsibly, and whether accountability mechanisms are in place before AI is used in high-impact areas such as health, finance, social protection, education, transport, policing or telecommunications. In practice, a preparedness diagnostic serves as a policy navigation tool: it can help governments to prioritize reforms, target investments, design capacity-building programmes, strengthen regulatory cooperation and determine which AI use cases are ready to scale and which require additional safeguards. Several global, regional and institution-specific initiatives demonstrate that AI preparedness can be assessed systematically and with increasing comparability, although these initiatives differ in their purpose, unit of analysis and methodology.

- At the government level, the Oxford Insights **Government AI Readiness Index 2025** remains a well-known transnational benchmark, assessing 195 governments on their capacity to harness AI for public benefit and focusing on public-sector capability, governance and the broader enabling ecosystem.⁵⁶ The IMF **AI Preparedness Index (API)** applies a macro-structural lens across 174 economies, examining digital infrastructure, human capital, labour market policies, innovation, economic integration and regulation/ethics.⁵⁷ The UNESCO **Readiness Assessment Methodology (RAM)** is not a ranking table but rather a country diagnostic tool for assessing preparedness for ethical and human-centred AI across five dimensions: legal and regulatory, social and cultural, scientific and

⁵⁶ Oxford Insights, Government AI Readiness Index 2025, <https://oxfordinsights.com/ai-readiness/government-ai-readiness-index-2025/>.

⁵⁷ International Monetary Fund (IMF), "Mapping the world's readiness for artificial intelligence shows prospects diverge", <https://www.imf.org/en/blogs/articles/2024/06/25/mapping-the-worlds-readiness-for-artificial-intelligence-shows-prospects-diverge>.

educational, economic, and technical/infrastructural.⁵⁸ The ITU report, **AI Ready - Analysis Towards a Standardized Readiness Framework**, similarly advances a structured approach to assessing readiness, proposing assessment criteria such as AI literacy, infrastructure and digital maturity, data ecosystems, policy and regulation, skills and education and ethics and responsibility.⁵⁹ The OECD has now also moved beyond observatory-style monitoring to a formal **OECD.AI Index**, designed as a composite framework for measuring national AI capabilities and tracking progress in implementing the OECD Recommendation on Artificial Intelligence.⁶⁰

- A second cluster of tools focuses on broader ecosystem benchmarking rather than direct preparedness scoring. **Stanford HAI AI Index** is a comprehensive evidence base covering AI research, talent, technical performance, investment, policy and societal impacts rather than a single government-preparedness scorecard.⁶¹ At the regional level, the European Commission **AI Watch**⁶² plays a similar role for Europe: it monitors the development, uptake and impact of AI, as well as policy initiatives and industrial/research capacity of AI across the European Union and Member States, making it especially useful for comparative regional diagnostics and policy tracking. OECD.AI broader observatory tools, policy navigator and classification framework likewise complement preparedness indices by helping policy-makers connect ecosystem conditions, policy implementation and risk/governance considerations.
- A third cluster focuses on organizational or implementation preparedness rather than national preparedness. The Cisco **AI Readiness Index** assesses enterprises and public-sector organizations across areas such as strategy, infrastructure, data, talent, governance and culture, providing an insight into whether institutions are operationally prepared to deploy AI.⁶³ The World Bank has recently added an important public-sector implementation perspective through **Building Trustworthy Artificial Intelligence: Frameworks, Applications and Self-Assessment for Readiness**, which focuses specifically on whether government agencies are ready to implement AI in a trustworthy and responsible manner.⁶⁴ These tools are valuable because they shift attention from national ambition and ecosystem conditions to institutional execution, an aspect that many country-level indices do not fully capture.

These instruments show that “AI preparedness” is now best understood as a family of related but distinct assessment approaches: **(i)** national ecosystem preparedness and competitiveness, **(ii)** public-sector and regulatory preparedness, **(iii)** organizational adoption and implementation maturity, and **(iv)** responsible or trustworthy AI governance preparedness. Any sound preparedness framework should therefore draw selectively from all of them rather than rely on a single scorecard. In practice, the strongest composite approaches now combine indicators on strategy and leadership, data and digital infrastructure, skills and talent, research and innovation capacity, institutional coordination, legal and regulatory preparedness, ethics and accountability, and implementation capacity within public institutions.

These resources provide essential reference points and demonstrate that AI preparedness is multidimensional and measurable. However, they are not tailored to the specific operational

⁵⁸ UNESCO, Readiness Assessment Methodology, <https://www.unesco.org/ethics-ai/en/ram>.

⁵⁹ International Telecommunication Union (ITU), “AI Ready: Analysis Towards a Standardized Readiness Framework”, https://www.itu.int/dms_pub/itu-t/opb/ai4g/T-AI4G-AI4GOOD-2025-6-PDF-E.pdf.

⁶⁰ OECD, AI Observatory Index, https://www.oecd.org/en/publications/oecd-ai-observatory-index_32c01014-en.html.

⁶¹ Stanford Institute for Human-Centered Artificial Intelligence (HAI), AI Index, <https://hai.stanford.edu/ai-index>.

⁶² European Commission, AI Watch, https://ai-watch.ec.europa.eu/index_en.

⁶³ Cisco, AI Readiness Index, https://www.cisco.com/c/m/en_us/solutions/ai/readiness-index.html.

⁶⁴ World Bank, World Development Report 2021: Data for Better Lives, <https://openknowledge.worldbank.org/entities/publication/835c80aa-0a3b-40c4-824e-d8d6ed831e98>.

and policy responsibilities of competent authorities tasked with implementing AI policy and regulation.

To address the gap, this guide aligns with the ITU AI Readiness Framework (Report 2.0, Jan 2026). Regulators can also leverage the ITU AI Readiness Enablement Toolkit (AI-RE Toolkit), which uses a foundational model derived from the ITU AI Readiness Knowledge Base. This allows policy-makers to move beyond static indices and conduct dynamic self-evaluations that identify "compound gaps" interconnected deficiencies in which weaknesses in one area, such as digital skills, can amplify challenges in another, such as AI oversight.

The diagnostic proposed in this guide builds on these global frameworks by translating broad dimensions into concrete questions, maturity levels and indicators that can be used by an AI authority, where established, a telecommunications or ICT regulator, a data protection authority, a digital ministry, a sector regulator for health or finance, or a provincial or city government. It is explicitly designed to inform real decisions: whether to proceed with an AI deployment in a high-risk domain; how to sequence legal reforms and capacity-building; where to invest in infrastructure and data systems; which regulatory coordination mechanisms to establish; and how to design procurement frameworks and transparency measures. The diagnostic is iterative and can be repeated every two to three years to monitor progress and adjust strategies.

Box 1: Use cases of AI preparedness diagnostics to implement policies and regulations

Experience from diverse jurisdictions shows that AI preparedness diagnostics are increasingly being used at the national level to translate AI ambition into practical implementation. These diagnostics do not always use the same terminology. They may be referred to as AI readiness or preparedness assessments, national AI landscape assessments, public-sector self-assessments, regulatory sandboxes, or institutional mapping exercises. What they all have in common is that they help governments to answer a practical implementation question: is the country actually ready to govern, procure, deploy, supervise and scale AI responsibly?

Some countries have used AI preparedness assessments to support national policy development and institutional reform. In Kenya, for example, the Artificial Intelligence Readiness Assessment Report examined the country's preparedness for ethical and responsible AI adoption, including legal and regulatory foundations, institutional coordination, infrastructure, skills and innovation capacity. Kenya is a useful example because it has a dynamic digital economy and active technology sector that needs to address practical implementation questions around regulatory capacity, data protection, inclusion and responsible deployment in public services.¹ In Montenegro, the United Nations Development Programme (UNDP) AI Landscape Assessment examined institutional readiness for ethical and strategic AI use, identifying opportunities to integrate AI into public services while also highlighting gaps in infrastructure, data interoperability, skills, inclusion and governance. This illustrates how a diagnostic can help a government move from general interest in AI to a sequenced implementation agenda.²

¹ UNESCO, Kenya: Artificial Intelligence Readiness Assessment Report, UNESCO Digital Library, 2025, <https://unesdoc.unesco.org/ark:/48223/pf0000392693>.

² United Nations Development Programme (UNDP), "Montenegro. Artificial Intelligence Landscape Assessment (AILA)", <https://www.undp.org/montenegro/publications/artificial-intelligence-landscape-assessment-aila>.

The Netherlands Artificial Intelligence Readiness Assessment Report, published by UNESCO, shows that preparedness diagnostics are relevant even for high-capacity jurisdictions. Although the Netherlands has a strong digital infrastructure and mature regulatory institutions, the assessment nevertheless examined how existing laws, institutional arrangements, public-sector AI use, research capacity and trust mechanisms need to adapt to AI. An important lesson here is that “AI preparedness” includes more than just ensuring basic connectivity or the existence of an AI strategy. Even advanced jurisdictions need diagnostics to identify coordination gaps, implementation risks and areas where existing regulators must adjust to AI-specific challenges.¹

An example from Bangladesh illustrates how a readiness assessment can support policy development in a rapidly digitalizing country. The AI readiness process was designed to provide a national picture of preparedness for responsible AI adoption and to support longer-term planning as Bangladesh develops its national AI policy and strengthens digital governance frameworks. This example is especially relevant for countries where political interest in AI is high, but significant constraints remain in infrastructure, data governance, institutional capacity and skills. In such contexts, a diagnostic can help governments avoid adopting ambitious AI policies without first identifying the foundations needed for effective implementation.²

Tanzania provides another example from a developing-country context. The Artificial Intelligence Readiness Assessment Report for Tanzania was developed through collaboration among national stakeholders and AI experts. It is useful because it demonstrates how a preparedness diagnostic can support countries exploring AI opportunities in development sectors assess whether governance frameworks, technical capacity, data systems, institutional coordination and safeguards are sufficiently developed before AI systems are scaled.³

The ITU report Uganda National AI Landscape Assessment, provides a practical diagnostic of Uganda’s AI preparedness, examining key gaps and opportunities across policy, regulation, infrastructure, data governance, skills, institutional capacity and risk management. Drawing on surveys, stakeholder consultations and international benchmarking, it sets out actionable recommendations to support responsible, inclusive and development-oriented AI adoption.⁴

Small states and island economies also benefit from this type of diagnostic. In Curaçao, the Artificial Intelligence Readiness Assessment Report demonstrates how readiness assessments can help smaller jurisdictions prioritize scarce resources, clarify institutional responsibilities, identify regulatory and technical gaps, and determine where regional cooperation or external expertise may be needed. For small states, the value of the diagnostic lies not in producing a large national AI bureaucracy, but in helping decision-makers sequence realistic reforms and partnerships.⁵

¹ UNESCO, The Netherlands: Artificial Intelligence Readiness Assessment Report, UNESCO Digital Library, 2025, <https://unesdoc.unesco.org/ark:/48223/pf0000393240>.

² UNESCO, Bangladesh: Artificial Intelligence Readiness Assessment Report, UNESCO Digital Library, 2026, <https://unesdoc.unesco.org/ark:/48223/pf0000396493>.

³ United Nations, Tanzania: Artificial Intelligence Readiness Assessment Report, 2025, <https://tanzania.un.org/en/297619-artificial-intelligence-readiness-assessment-report>.

⁴ International Telecommunication Union (ITU), National Artificial Intelligence Landscape Assessment and Implementation Framework for Uganda, 2025, <https://www.itu.int/hub/publication/d-uga-naaila-2025/>.

⁵ UNESCO, Curaçao: Artificial Intelligence Readiness Assessment Report, UNESCO Digital Library, 2025, <https://unesdoc.unesco.org/ark:/48223/pf0000394952>.

Regulatory sandboxes can also function as practical preparedness diagnostics. Spain provides a strong example. Through its AI regulatory sandbox, the Government of Spain tested high-risk AI systems under supervised conditions before full implementation of the EU AI Act. The experience informed practical guides for AI Act compliance, including guidance on risk management, data governance, transparency, human oversight, robustness, cybersecurity and technical documentation. This shows how a diagnostic exercise can move beyond assessing abstract readiness and test whether firms, regulators and public authorities understand what compliance requires in practice.¹

These examples show that AI preparedness diagnostics are not merely abstract benchmarking exercises and should not be associated with a single organization or methodology. They include global indices, national landscape assessments, public-sector self-assessments, sector-specific diagnostics, sandboxes and institutional mapping exercises. In advanced regulatory environments, such as Spain and the Netherlands, they help to translate legal obligations into guidance, institutional mandates and supervisory tools. In emerging digital economies, such as Kenya, Bangladesh and Tanzania, they help to identify the infrastructure, data governance, skills and regulatory capacities required prior to scaling AI. In smaller economies, such as Curaçao, they help to prioritize scarce resources and determine where shared capacity or partnerships may be necessary.

¹ Spanish Agency for the Supervision of Artificial Intelligence (AESIA), Practical guides for AI Act compliance, <https://aesia.digital.gob.es/en/present/resources/practical-guides-for-ai-act-compliance>.

For this guide, the practical lesson is clear: AI preparedness diagnostics should be used as implementation instruments. They help policy-makers and regulators to determine which AI reforms are feasible immediately, which require prior investment, which institutions must coordinate, which safeguards are missing, and which high-risk use cases should not be scaled until minimum conditions are in place. The diagnostic therefore serves as a bridge between AI policy and AI delivery. It turns ambition into sequencing, coordination into action, and broad principles into practical governance reforms.

AI preparedness as development and innovation policy

AI preparedness diagnostics should be understood not only as governance tools, but also as development and innovation policy tools. The United Nations Conference on Trade and Development (UNCTAD) 2025 Technology and Innovation Report frames AI policy as part of a broader industrial and innovation agenda, emphasizing that countries need to support both the adoption of AI across existing sectors and the development of national capabilities for AI innovation.⁶⁵ This is especially important for developing countries, where AI strategies may remain declarative unless they are backed by resources, implementation instruments, infrastructure, data systems, skills and ecosystem coordination. A preparedness diagnostic helps policy-makers to test whether AI ambition is matched by the practical foundations needed for inclusive development, productivity growth and strategic autonomy.

⁶⁵ United Nations Conference on Trade and Development (UNCTAD), 2025 Technology and innovation report, <https://unctad.org/publication/technology-and-innovation-report-2025>.

3.2 The eight policy-relevant preparedness dimensions

The AI preparedness diagnostic is structured around eight policy-relevant preparedness dimensions that correspond directly to the core tasks of collaborative AI frameworks and that emerge consistently from global preparedness literature and country practice. It reflects the three leverage points highlighted in the UNCTAD Technology and Innovation Report 2025 for national AI policy: infrastructure, data and skills. Infrastructure determines whether AI can be deployed reliably and equitably; data systems determine whether AI can be developed and used responsibly; and skills determine whether AI adoption can spread beyond a narrow technical elite. These foundations cut across the eight preparedness dimensions and help to ensure that AI governance is linked to real implementation capacity. These dimensions are:

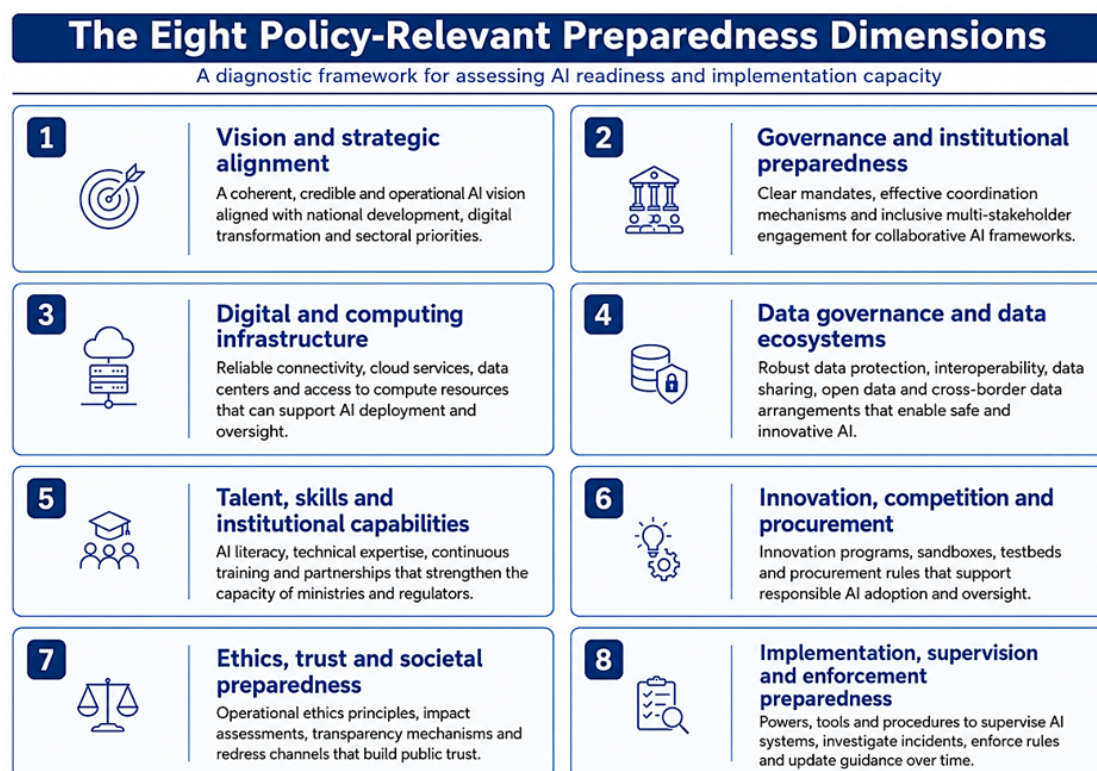
1. **Vision and strategic alignment.** This dimension looks at whether the country or jurisdiction has a coherent, credible and operationalized AI vision that aligns with broader development, digital transformation and sectoral objectives and that assigns roles, responsibilities and resources for implementation.
2. **Governance and institutional preparedness for collaborative AI frameworks.** This dimension looks at whether mandates for AI-relevant issues (data protection, telecoms, competition, consumer, sector regulation and cyber) are clear; whether coordination mechanisms (AI councils, inter-agency working groups and memoranda of understanding) exist and function; and whether multi-stakeholder engagement (with academia, industry and civil society) is structured and inclusive.
3. **Digital and computing infrastructure.** This dimension looks at whether connectivity 4G/5G, (high speed fixed and wireless broadband), cloud services, data centres, access to compute resources (graphics processing units (GPUs), high-performance computing), and electricity/energy are adequate, reliable and inclusive enough to support AI deployment and regulatory oversight.
4. **Data governance and data ecosystems.** This dimension looks at whether data protection law and enforcement are robust; whether open data, data sharing and interoperability frameworks exist; and whether data classification, privacy-enhancing technologies and cross-border data flow arrangements support safe and innovative AI.
5. **Talent, skills and institutional capabilities.** This dimension looks at whether regulators and ministries possess AI and data literacy, employ technical staff or have structured access to expertise; whether continuous training and education programmes exist; and whether partnerships with universities and research institutes support AI governance and foresight.
6. **Innovation, competition and procurement preparedness.** This dimension looks at whether innovation programmes, regulatory sandboxes and testbeds support responsible AI development;⁶⁶ whether competition authorities address AI-related risks (including algorithmic collusion and dark patterns); and whether procurement frameworks include AI-specific governance requirements (including transparency, access to documentation, audit rights, interoperability and exit clauses).
7. **Ethics, trust and societal preparedness.** This dimension looks at whether AI ethics guidelines or principles are adopted and operationalized; whether AI impact assessments

⁶⁶ Regulatory sandboxes and testbeds are included under Innovation and procurement preparedness because their primary function is to help governments, regulators, firms and researchers test AI systems, business models and deployment conditions in controlled environments before wider market or public-sector use. While they often require strong institutional coordination, which links them to Dimension 2, their operational purpose is innovation-related: they help to identify technical, legal, ethical, consumer protection and safety issues early; generate evidence for future rules or guidance; and support responsible AI development without prematurely blocking experimentation. For this reason, the diagnostic assesses sandboxes and testbeds under Dimension 6, alongside innovation programmes and AI-ready procurement frameworks. Dimension 2 focuses more specifically on the institutional architecture needed for collaborative AI governance, including mandates, coordination mechanisms and stakeholder engagement.

or human rights impact assessments are used for high-risk systems; and whether transparency mechanisms (such as public registers of algorithms) and redress channels exist.

8. **Implementation, supervision and enforcement preparedness.** This dimension looks at whether competent authorities have powers, tools and procedures to supervise AI systems, investigate complaints and incidents, impose corrective measures and sanctions, and participate in cross-border enforcement cooperation; and whether AI-related rules and guidance are regularly evaluated and updated.

Figure 5: The eight policy-relevant preparedness dimensions



Source: ITU

Each dimension is assessed using plain-language indicators and qualitative maturity levels, as detailed in Part 4.

3.3 Step-by-step methodology for performing the diagnostic

The diagnostic can be performed at the national or subnational level using a structured six-step process. This process is designed to combine document review, stakeholder interviews and institutional self-assessment into a coherent, actionable picture of preparedness, and can be adapted to contexts ranging from low-capacity environments with limited data to high-capacity environments with extensive documentation and indices.

Figure 6: AI preparedness assessment – six-step process



Source: ITU

Step 1: Define objectives and scope

The first step is to articulate why an AI preparedness diagnostic is being performed and what decisions it should inform. Clarity on objectives shapes the entire process. Objectives typically include:

- **Policy and strategy formulation.** Supporting the drafting or revision of a national AI strategy, digital policy or sectoral AI action plan.
- **Legal and regulatory development.** Preparing to design or implement AI-specific legislation or amendments to data, telecoms, consumer or sector-specific laws.
- **Deployment decisions for high-risk AI systems.** Assessing whether suitable conditions exist to deploy or scale AI in high-risk domains such as social protection, health or policing.
- **Institutional coordination and capacity-building.** Strengthening collaboration among regulators and ministries, identifying capacity gaps and prioritizing training and institutional reforms.

The scope may be whole-of-government, sectoral (telecommunications, financial services, health, education or justice), whole-of-society or subnational (a province, state, or large city), depending on the objective. The results, level of detail, timeline and expected outputs (such as internal briefings, public reports, roadmaps or draft legislative packages) should be documented in a short terms of reference, endorsed by relevant political or institutional leadership to secure commitment and resource allocation.

Step 2: Establish a diagnostic governance team

The second step is to establish a small, empowered diagnostic governance team to coordinate evidence collection, analysis and reporting. This team is typically chaired by a central authority responsible for digital or AI policy, such as:

- a digital or ICT ministry
- a central digital transformation authority
- a national AI coordination body.

Membership commonly includes:

- the telecommunications/ICT regulator
- the national data protection authority
- competition and consumer protection agencies
- the national cybersecurity authority or computer emergency response team (CERT)
- one or two key sector regulators or ministries relevant to the chosen diagnostic focus (for example, health, finance, education and social protection).

The terms of reference for the team should specify roles in evidence collection, facilitation of interviews and workshops, analysis and drafting, and should set out mechanisms for requesting information, sharing drafts and resolving disagreements. Where a national AI council or inter-ministerial committee already exists, the diagnostic team can report to or work under this body to ensure alignment with broader AI policy processes.

Step 3: Collect evidence through document review, stakeholder interviews and self-assessment

The third step is to collect evidence using three complementary lenses.

Document and data review should cover:

- AI-specific laws and regulations, where these exist;
- Cross-cutting frameworks relevant to AI: data protection and privacy laws, telecommunications and electronic communications laws, cyber and consumer protection laws, competition law provisions on algorithmic practices;
- Sector-specific frameworks in high-risk domains: health (for example, medical devices regulation in the European Union, digital health regulations in the United States and India), financial services (for example, national fintech and digital credit rules), education (for example, AI in exams and grading), social protection and justice;
- National and sectoral strategies: AI strategies (for example, the national AI strategy in Canada⁶⁷, the national AI policy⁶⁸ in Rwanda, the national AI strategy⁶⁹ in Egypt and the national AI strategy⁷⁰ in the United Arab Emirates), digital strategies, sectoral AI plans and human rights or development plans;
- Institutional documents: regulators' strategic plans, guidance and enforcement reports, government audit reports and court decisions relevant to AI;
- Existing diagnostics and indices.

⁶⁷ Government of Canada, Innovation, Science and Economic Development Canada, "Canada's National Artificial Intelligence Strategy: AI for All", <https://ised-isde.canada.ca/site/ised/en/canadas-national-artificial-intelligence-strategy-ai-all>.

⁶⁸ For information on the Rwanda Government AI policy, see the website of the Ministry of ICT and Innovation, Republic of Rwanda, <https://www.minict.gov.rw/ai-policy>.

⁶⁹ National Council for Artificial Intelligence, Arab Republic of Egypt, Egypt National Artificial Intelligence Strategy, Second Edition (2025-2030), January 2025, <https://ai.gov.eg/SynchedFiles/en/Resources/AIstrategy%20English%2016-1-2025-1.pdf>.

⁷⁰ Government of the United Arab Emirates, UAE National Strategy for Artificial Intelligence 2031, 2018, <https://staticcdn.mbzuai.ac.ae/mbzuaiwpprd01/2022/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.pdf>.

Stakeholder interviews use semi-structured guides to elicit qualitative insights from:

- Senior officials in ministries and regulators with responsibility for AI, data, telecommunications, competition, consumer protection, cyber and key sectors;
- Technical staff running AI and data projects in government, including those working on digital identity, payments, health information systems, agricultural platforms and telecommunication networks;
- Representatives of telecommunications operators, digital service providers, AI developers, SMEs and industry associations;
- Civil society organizations (for example, digital rights non-governmental organizations (NGOs), consumer associations and labour unions) and human rights institutions;
- Academics and think tanks engaged in AI governance research.

Institutional self-assessment invites each participating institution to rate its maturity on each preparedness dimension, using a simple four-level scale, and to provide concrete examples and evidence to justify the rating. This can be done using a standardized template aligned with the eight dimensions. For example, a data protection authority may rate itself as "emerging" or "established" on data governance and enforcement preparedness, citing specific cases and guidance, while a telecommunications regulator may rate itself "nascent" on AI-specific oversight.⁷¹

Triangulating document reviews, stakeholder interviews and self-assessments helps to mitigate biases and reveals discrepancies. For instance, an agency may self-assess as "established" on AI enforcement but documents and interviews might show few AI-related cases and limited technical expertise, suggesting a need for capacity-building and more realistic self-perception.

Step 4: Apply diagnostic indicators and qualitative maturity scoring

The fourth step involves structured workshops during which the diagnostic governance team and relevant institutions review evidence for each dimension and agree on a maturity level. A uniform, four-level qualitative scale is used across all dimensions:

- **Level 1: Nascent.** Policies, institutions or practices are largely absent or ad hoc; awareness of AI implications is low; coordination is minimal; and there is little or no formal supervision of AI-specific risks.
- **Level 2: Emerging.** Basic frameworks or initiatives exist but are incomplete or inconsistently implemented; coordination is limited; pilots are under way; some guidance or policies mention AI but these have not been fully operationalized.
- **Level 3: Established.** Coherent frameworks and institutions are in place; coordination is regular; procedures are documented; supervision and reporting occur in practice; and AI-related risks are addressed in a structured way in several sectors.
- **Level 4: Advanced.** Systems are comprehensive, adaptive and well-resourced; collaboration is robust; supervision is risk-based and proactive; policies and practices are regularly evaluated and refined; and the jurisdiction participates in shaping regional or global AI governance.

⁷¹ Informed by self-assessment frameworks, such as this preparedness framework and the Cisco AI Readiness Index, 2024, available at https://www.cisco.com/c/dam/m/en_us/solutions/ai/readiness-index/2024-m11/documents/cisco-ai-readiness-index.pdf.

Step 5: Synthesize findings and identify priority gaps

In the fifth step, findings across all eight dimensions are synthesized to provide a consolidated picture of overall preparedness. Visualization tools, such as radar or spider charts, can be used to show maturity scores for each dimension, highlighting any imbalances.

For example, a country might score:

- Level 3: Established on vision and strategic alignment (clear AI strategy and sector plans);
- Level 2: Emerging on governance and institutional coordination (coordination body exists but is weak);
- Level 3: Established on infrastructure (reliable connectivity and data centres);
- Level 2: Emerging on data governance (recent data protection law with limited enforcement);
- Level 1: Nascent on skills (few AI experts in government);
- Level 2: Emerging on innovation and procurement (some sandboxes and generic procurement rules);
- Level 2: Emerging on ethics and trust (ethics guidelines exist but limited operationalization);
- Level 1: Nascent on implementation and enforcement (few AI-specific cases and limited tools).

This high-level view enables decision-makers to identify strengths and weaknesses, providing a basis for priority setting. These priorities should take into account the severity of the risks, particularly in sectors where high-risk AI systems are already being deployed or where deployment is planned, such as welfare eligibility, policing and health diagnostics. They should also consider the dependencies between different dimensions – for example, recognizing that effective enforcement relies on strong governance, robust data systems and adequate skills. In addition, priorities should be assessed for their feasibility within a 12–24 month time-frame, taking into account political, budgetary and technical constraints, while also aligning with ongoing reforms and international commitments (such as EU AI Act implementation timelines, data protection obligations and digital trade agreements).

Step 6: Develop a roadmap and early actions

In the sixth step, the diagnostic is translated into a roadmap of actions for each dimension, with clear responsibilities, timelines and resource implications. Actions may include:

- **Legal and policy measures:** drafting or updating AI strategies; embedding AI into sectoral strategies; and adopting or amending AI, data, telecoms, or consumer laws to reflect AI-specific issues (for example, clarifying definitions of AI systems, high-risk uses, responsibilities of providers and deployers).
- **Institutional measures:** establishing or formalizing AI councils or coordination bodies; defining or clarifying mandates for data protection, telecoms, competition and sector regulators; creating AI or data units within key agencies; and setting up expert advisory groups or centres of excellence.
- **Infrastructure and data investments:** improving reliable connectivity, especially in rural and underserved areas; adopting secure government cloud strategies; creating data-sharing

frameworks and curated datasets for AI with robust safeguards; and participating in regional high-performance computing (HPC) initiatives such as EuroHPC.⁷²

- **Capacity-building and skills development:** designing and delivering AI governance training for civil servants, regulators and judges; establishing AI fellowship programmes and secondments with universities and research institutes; and supporting AI-related curricula in universities and technical institutes.
- **Innovation and procurement instruments:** launching or expanding AI sandboxes and testbeds in priority sectors, involving regulators as learning partners; updating procurement templates to include AI-specific clauses (transparency, access to logs and documentation, audit rights, security and exit provisions); and supporting responsible AI innovation through grants and challenges.
- **Ethics, transparency and trust mechanisms:** adopting or updating AI ethics guidelines (informed by the UNESCO Recommendation on the Ethics of Artificial Intelligence⁷³); introducing AI impact assessments or human rights impact assessments for high-risk systems; and creating public registers of AI and algorithmic systems used in government.
- **Supervision and enforcement steps:** developing AI-adapted supervision methods (algorithm audits, testing frameworks such as AI Verify; undertaking first thematic reviews or investigations of AI systems in specific sectors; and joining cross-border enforcement networks (for example, the Global Privacy Assembly).

Early actions focus on high-impact, feasible measures that can build momentum and demonstrate commitment, while more complex reforms are sequenced over several years.

4 Diagnostic components by preparedness dimension: Questions, maturity levels and indicators

AI preparedness is not determined by the existence of a national AI strategy alone. A jurisdiction may have a strong policy vision but lack the institutional coordination, data governance, infrastructure, skills, procurement tools, ethical safeguards or supervisory capacity needed to implement that vision in practice. Conversely, a country may have strong digital infrastructure or innovation capacity but lack the governance mechanisms needed to ensure that AI systems are trustworthy, inclusive, safe and aligned with public interest objectives.

The diagnostic is structured around the eight preparedness dimensions (each containing seven indicators, scoring on a scale of 0 to 2, with a maximum of 14 points for each of the dimensions):

- Dimension 1: Vision and strategic alignment
- Dimension 2: Governance and institutional preparedness
- Dimension 3: Digital and computing infrastructure
- Dimension 4: Data governance and data ecosystems
- Dimension 5: Talent, skills and institutional capabilities
- Dimension 6: Innovation, competition and procurement
- Dimension 7: Ethics, trust and societal preparedness
- Dimension 8: Implementation, supervision and enforcement preparedness.

⁷² European High Performance Computing Joint Undertaking (EuroHPC JU), https://www.eurohpc-ju.europa.eu/index_en

⁷³ UNESCO, Recommendation on the Ethics of Artificial Intelligence, 2021, <https://unesdoc.unesco.org/ark:/48223/pf0000381137>

Scoring methodology

The scoring process should include the following steps:

- **Step 1: Score each indicator.** Each dimension contains seven indicators. Each indicator is scored on a 0–2 scale based on the evidence available.
- **Step 2: Calculate the dimension score.** Each dimension has a maximum score of 14 points.
- **Step 3: Establish a maturity level.** The score for each dimension is converted into one of four maturity levels: Nascent, Emerging, Established or Advanced.
- **Step 4: Calculate the overall preparedness score.** Scores across all eight dimensions are added to produce an overall score out of 112.

Each indicator is scored using a three-point scale.

Score	Assessment	Description
0	Not Present	No evidence exists.
1	Partially present	The indicator exists in draft/pilot/partial/fragmented/ or limited form, but implementation is incomplete, inconsistent, under-resourced or not yet institutionalized.
2	Fully present	The indicator is formally established/operational/adequately resourced/applied in practice and supported by evidence of implementation.

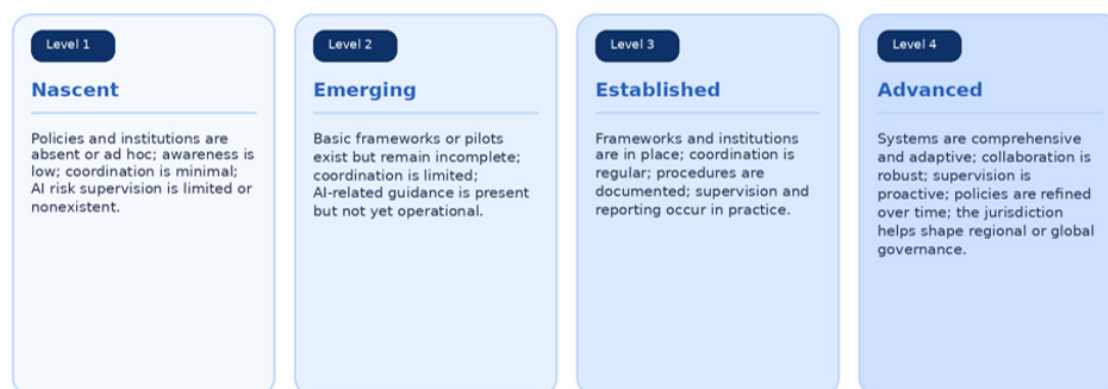
The maximum score for each dimension is 14 points (total scores of the seven indicators).

Dimension score

Dimension score	Maturity level
0–3	(Level 1) Nascent
4–7	(Level 2) Emerging
8–11	(Level 3) Established
12–14	(Level 4) Advanced

Maturity levels

As defined in Chapter 3, the uniform, four-level qualitative maturity scale is reflected for ease of reference in Figure 7 below.

Figure 7: Maturity levels

Overall preparedness score

The overall preparedness score is calculated by adding the scores across all eight dimensions. However, the overall score is indicative only, as the greater value lies in the scores for each dimension and, in particular, its indicators, which help to identify strengths and gaps and determine where efforts should be focused to address the gaps identified.

Maximum possible score: **8 dimensions × 14 points = 112 points**

Overall score	Overall preparedness level
0-28	(Level 1) Nascent
29-56	(Level 2) Emerging
57-84	(Level 3) Established
85-112	(Level 4) Advanced

Summary of the formula

- Dimension score = Sum of the seven indicator scores.
- Overall preparedness score = Sum of all eight dimension scores.
- This scoring approach creates a clear chain from evidence to assessment: *Evidence* → *Indicator score* → *Dimension score* → *Dimension maturity level* → *Overall preparedness score*.

4.1 Dimension 1: Vision and strategic alignment

This dimension assesses whether the jurisdiction has a coherent, credible and implementable AI vision aligned with broader development objectives. It examines whether AI is treated as a strategic policy priority rather than a collection of isolated pilots. A strong score in this dimension means that AI objectives are linked to national development goals, digital transformation agendas, sector strategies, institutional responsibilities, budgets, implementation plans and monitoring arrangements.

Indicator	Score = 0 Not present	Score = 1 Partially present	Score = 2 Fully present	Score
1. AI strategy framework	No formal national AI strategy or equivalent policy framework exists.	A draft AI strategy exists, or AI objectives are mentioned in broader digital, data, innovation or sector strategies.	A formal AI strategy or equivalent policy framework has been adopted and is publicly available.	
2. Strategic integration	AI is not reflected in national development, digital transformation or sector planning.	AI is referenced in selected plans or sectors but is not consistently integrated across government priorities.	AI objectives are integrated into national development plans, digital transformation strategies and relevant sector strategies.	
3. Opportunity and risk coverage	Policies do not address AI risks or opportunities.	Policies address some AI opportunities and risks, but coverage is incomplete or uneven.	Policies address AI opportunities such as growth, efficiency, innovation and inclusion, as well as risks related to rights, safety, security, discrimination and environmental impacts.	
4. Institutional ownership	No institutions are clearly responsible for AI strategy implementation.	Some responsibilities are assigned, but roles remain unclear, overlapping or poorly understood.	Institutional responsibilities are clearly assigned.	
5. Implementation readiness	No implementation framework exists.	An implementation framework or roadmap exists but lacks detail, sequencing or operational clarity.	A time-bound implementation framework exists with milestones, lead institutions and implementation mechanisms.	
6. Resource commitment	No budget or resources have been allocated for AI strategy implementation.	Some project-based or donor-supported funding exists, but resources are incomplete or uncertain.	Dedicated budgets, financial resources or investment plans have been identified for AI implementation.	
7. Monitoring and reporting	No monitoring, evaluation or reporting mechanism exists.	Limited monitoring or reporting exists, but it is irregular or not linked to strategy implementation.	Regular monitoring, reporting, review and updating mechanisms are in place.	

Maturity levels

Dimension score	Level	Description
0-3	(Level 1) Nascent	AI is mentioned sporadically in policy documents but there is no strategy or implementation plan, and no assigned responsibilities or funding exist.
4-7	(Level 2) Emerging	AI objectives are present in digital or sector strategies, or a draft AI strategy exists, but implementation details, budgets, responsibilities and monitoring remain unclear.
8-11	(Level 3) Established	A dedicated AI strategy or equivalent framework exists with clear goals, responsible institutions, time-bound implementation arrangements, basic funding and monitoring.
12-14	(Level 4) Advanced	AI strategy is integrated across sectors and aligned with development priorities; implementation is funded, monitored, publicly reported and periodically updated based on evaluation and stakeholder input.

4.2 Dimension 2: Governance and institutional preparedness for collaborative AI frameworks

This dimension assesses whether institutional arrangements can support collaborative AI governance. AI systems cut across legal mandates and policy domains, including data protection, telecommunications, competition, consumer protection, cybersecurity, public procurement and sector regulation. Effective governance therefore depends on clear mandates, coordination mechanisms, regulatory cooperation, stakeholder engagement and international collaboration.

Indicator	Score = 0 Not present	Score = 1 Partially present	Score = 2 Fully present	Score
1. AI coordination structures	No AI coordination body, working group, council or equivalent mechanism exists.	An informal working group or coordination mechanism exists but has limited authority, unclear membership or irregular activity.	A formal AI coordination body exists with defined mandate, membership, procedures and outputs.	
2. Institutional mandates	Mandates for AI-relevant issues are absent.	Some mandates have been defined, but overlaps remain across institutions.	Roles and responsibilities are clearly defined.	
3. Inter-agency coordination	No structured mechanisms for inter-agency coordination on AI exist.	Coordination occurs on an ad hoc basis through meetings, consultations or informal exchanges.	Formal inter-agency mechanisms exist, including working groups, memoranda of understanding, joint committees and shared protocols.	

(continued)

Indicator	Score = 0 Not present	Score = 1 Partially present	Score = 2 Fully present	Score
4. Operational collaboration	Coordination does not produce joint outputs or practical results.	Some joint activities or outputs exist, but they are irregular or limited.	Coordination produces regular outputs, such as joint guidance, action plans, policy papers, implementation decisions or shared tools.	
5. Regulatory cooperation	Regulators operate independently and do not coordinate on AI-related issues.	Some cooperation occurs between regulators, but it is issue-specific or informal.	Data protection, telecommunications, competition, consumer protection, cybersecurity and sector regulators actively cooperate on AI-related matters.	
6. Stakeholder engagement	Stakeholders are not meaningfully engaged in AI policy or regulatory processes.	Stakeholder consultations sometimes take place but are not systematic or well documented.	Academia, industry, startups, professional associations, civil society and affected groups participate regularly and meaningfully.	
7. International cooperation	The country does not participate in international or regional AI governance discussions.	Participation occurs occasionally but is not linked to domestic implementation.	The jurisdiction actively participates in regional or international AI governance, standards, safety or regulatory cooperation initiatives.	

Maturity levels

Dimension score	Level	Description
0-3	(Level 1) Nascent	No formal AI coordination body exists; collaboration is ad hoc; mandates are unclear or overlapping.
4-7	(Level 2) Emerging	A coordination body or informal working group exists, but it meets infrequently, has limited authority and produces few outputs.
8-11	(Level 3) Established	A coordination body with clear terms of reference, regular meetings, broad membership and documented outputs is in place; key regulators coordinate on AI issues.
12-14	(Level 4) Advanced	Collaborative AI governance is deeply embedded; coordination bodies exercise influence or decision-making authority; joint guidance, shared tools, stakeholder forums and cross-border cooperation are actively implemented.

4.3 Dimension 3: Digital and computing infrastructure

This dimension assesses whether the jurisdiction has the connectivity, cloud, data centre, compute, energy and resilience foundations needed to support AI deployment and oversight. AI systems depend on reliable digital infrastructure. Without adequate broadband, secure cloud environments, data centre capacity, compute resources, cybersecurity and energy reliability, AI adoption may remain limited, unequal or unsafe.⁷⁴

Indicator	Score = 0 Not present	Score = 1 Partially present	Score = 2 Fully present	Score
1. Connectivity readiness	Significant gaps exist in (fixed and wireless) broadband connectivity (no 4G/LTE, no 5G and limited fixed broadband).	Broadband connectivity is available in many areas but remains uneven in urban areas: 4G/LTE, 5G (in main cities) and fixed broadband.	High speed fixed and wireless broadband (4G and 5G) connectivity is available across the country.	
2. Cloud readiness	Public institutions do not use secure cloud services.	Some public institutions use cloud services, but cloud adoption is fragmented or lacks clear security and governance rules.	Secure public, private or hybrid cloud services are available and governed by clear cloud adoption and security policies.	
3. Data centre ecosystem	National or regional data centre capacity is absent.	Some data centre capacity exists, but resilience, security, geographic distribution, certification or governance remain limited.	Data centres are available, secure, resilient, appropriately governed and with sufficient capacity to support public sector digital services and AI workloads.	
4. Compute capacity	Public institutions have no access to AI compute, GPUs, HPC or cloud-based compute resources.	Limited compute resources are available to a small number of institutions, or through ad hoc partnerships.	AI compute resources, including GPUs, HPC, cloud-based compute, or regional compute arrangements, are accessible to relevant public institutions.	
5. Public sector infrastructure	Core public-sector digital systems not suitable for AI-enabled services.	Basic digital public systems exist, but their interoperability, scalability or security are limited.	Digital public infrastructure supports secure, interoperable and scalable AI-enabled public services.	

⁷⁴ ITU tools are available to conduct a more in-depth assessment of connectivity/infrastructure planning, taking into consideration a broader range of indicators, such as the [connectivity planning platform](#) (CPP).

(continued)

Indicator	Score = 0 Not present	Score = 1 Partially present	Score = 2 Fully present	Score
6. Resilience and energy reliability	Power outages, weak backup systems.	Some resilience and backup measures exist, but they are incomplete or limited to priority institutions.	Critical digital and AI systems are supported by reliable energy, backup power, redundancy, disaster recovery and service continuity arrangements.	
7. Infrastructure strategy	There is no strategy for aligning infrastructure with AI use cases or future workloads.	Infrastructure planning mentions AI but lacks detail on cloud, HPC, edge computing, data centres, energy or resilience.	Infrastructure planning explicitly anticipates AI workloads and addresses centralized, cloud-based, HPC and edge deployment needs.	

Maturity levels

Dimension score	Level	Description
0-3	(Level 1) Nascent	Major connectivity, energy, cloud and compute gaps exist; many public institutions lack reliable Internet, power or digital infrastructure.
4-7	(Level 2) Emerging	Connectivity and cloud use are improving, but compute access is limited, resilience is uneven and infrastructure planning does not systematically address AI needs.
8-11	(Level 3) Established	Widespread connectivity, functioning data centres, cloud strategies, compute access for core institutions, and basic resilience planning are in place.
12-14	(Level 4) Advanced	Infrastructure is high quality, secure, resilient, inclusive, and strategically designed for AI workloads, including cloud, HPC, edge computing and energy implications.

4.4 Dimension 4: Data governance and data ecosystems

This dimension evaluates whether data protection, data access, data quality, data sharing and stewardship practices support trustworthy and effective AI. AI systems require large quantities of reliable, representative, well-governed and lawfully processed data. Weak data governance can produce unsafe, biased, inaccurate or unlawful AI systems, while excessive fragmentation can prevent beneficial AI innovation and public-sector transformation.

Indicator	Score = 0 Not present	Score = 1 Partially present	Score = 2 Fully present	Score
1. Data protection framework	No modern data protection law or equivalent framework exists.	A data protection law exists but implementation, enforcement or AI relevance remains limited.	A modern data protection framework is in force and applies effectively to AI-relevant data practices.	
2. Data protection authority (DPA) capacity	No operational DPA or equivalent oversight body exists.	A DPA or oversight body exists but is under-resourced, lacks technical expertise or has limited AI-related activity.	The DPA is operational, independent, adequately resourced, technically capable and active on AI-related issues.	
3. Open data ecosystem	No public datasets are available, and open data practices are absent.	Open data portals or datasets exist, but quality, metadata, licensing, usability or uptake remain limited.	High-value public datasets are available in machine-readable form with clear metadata, licensing and active use by public institutions, researchers or innovators.	
4. Data-sharing governance	No structured mechanisms exist for data sharing within government, with private entities or across borders.	Data sharing occurs on an ad hoc basis or through limited agreements.	Formal data-sharing frameworks, agreements, and safeguards exist for government, private-sector and cross-border data sharing where appropriate.	
5. Data quality and stewardship	No clear standards exist for data quality, classification, metadata, stewardship or accountability.	Some data quality or classification practices exist but are inconsistent across institutions.	Data quality, classification, metadata, stewardship and accountability practices are established and applied across relevant institutions.	
6. Privacy safeguards	AI-related data processing does not use privacy safeguards.	Basic anonymization or de-identification practices are used in some projects.	Privacy safeguards such as anonymization, pseudonymization, privacy-enhancing technologies or synthetic data are systematically used where appropriate.	
7. AI data readiness	AI-relevant datasets are unavailable or inaccessible.	Some AI-relevant datasets are available, but access, quality, interoperability or safeguards remain limited.	AI-relevant datasets are accessible, high quality, interoperable, lawfully governed and usable for responsible innovation, research, supervision and service delivery.	

Maturity Levels

Dimension score	Level	Description
0-3	(Level 1) Nascent	No modern data protection framework or operational DPA exists; data practices are fragmented among institutions; AI-related data risks are poorly understood.
4-7	(Level 2) Emerging	Data protection and open data frameworks exist, but enforcement, data quality, sharing and AI-specific guidance remain limited.
8-11	(Level 3) Established	Data protection is enforced, open data is actively used, structured data-sharing agreements exist and AI projects incorporate privacy-by-design.
12-14	(Level 4) Advanced	A trusted, interoperable, privacy-preserving data ecosystem supports responsible AI innovation, supervision, cross-border data flows and continuous governance improvement.

4.5 Dimension 5: Talent, skills and institutional capabilities

This dimension examines whether public institutions have the human capital and organizational capacity needed to govern AI. AI preparedness requires not only technical experts but also policy-makers, regulators, lawyers, procurement officials, judges and public managers who understand AI risks, opportunities and governance tools. Without institutional capabilities, AI policy remains dependent on vendors, consultants or isolated individuals.

Indicator	Score = 0 Not present	Score = 1 Partially present	Score = 2 Fully present	Score
1. Public sector AI expertise	Ministries and public institutions lack staff with AI, data science or digital governance expertise.	Some institutions have isolated experts, but expertise is uneven and not institutionalized.	Relevant ministries and agencies have access to AI, data science, digital governance and data protection expertise.	
2. Regulatory technical capacity	Regulators lack technical expertise needed to assess AI systems or AI-related risks.	Some regulators have limited technical staff or external support, but capacity is uneven.	Regulators have internal or structured external technical capacity to assess AI-related issues.	
3. Institutional support mechanisms	No advisory boards, centres of excellence, fellowships, secondments or structured expert support exist.	Some support mechanisms exist but are ad hoc, donor-dependent or limited to selected institutions.	Structured support mechanisms such as advisory boards, centres of excellence, fellowship programmes, secondments or expert panels are available.	

(continued)

Indicator	Score = 0 Not present	Score = 1 Partially present	Score = 2 Fully present	Score
4. Professional development	No training exists on AI governance, data protection, algorithmic accountability or digital rights.	Occasional training activities are delivered but are not systematic or institutionalized.	Regular professional development programmes reach civil servants, regulators, judges and oversight bodies.	
5. Academic and research partnerships	Government has no meaningful partnerships with universities, research institutes or think tanks on AI.	Some partnerships exist but are informal or limited to isolated projects.	Structured partnerships support AI projects, evaluations, foresight, policy advice and capacity-building.	
6. Applied knowledge ecosystem	External expertise is not used, or the government relies entirely on vendors without developing independent capacity.	External experts are used occasionally, but knowledge transfer is limited.	External expertise is systematically used to support policy design, evaluation, audits, foresight and institutional learning.	
7. AI literacy and awareness	Non-technical officials and the wider public have little or no access to AI literacy initiatives.	Basic AI awareness activities exist but reach limited audiences.	AI literacy initiatives are available for non-technical public officials and the wider public.	

Maturity levels

Dimension score	Level	Description
0-3	(Level 1) Nascent	Public institutions have minimal AI awareness, little or no technical expertise, and rely heavily on vendors for AI knowledge.
4-7	(Level 2) Emerging	Isolated expertise, ad hoc training and some academic partnerships exist, but capacity remains uneven and dependent on external support.
8-11	(Level 3) Established	Dedicated AI or data units, regular training programmes, structured partnerships and some internal audit or analysis capabilities exist.
12-14	(Level 4) Advanced	Strong cross-disciplinary capacity exists across legal, technical, policy, regulatory, and ethical domains; institutions can develop, procure, supervise and evaluate complex AI systems.

4.6 Dimension 6: Innovation, competition and procurement

This dimension assesses whether innovation policies, regulatory sandboxes, testbeds, competition protection tools and public procurement frameworks support responsible AI development and deployment. Public procurement is especially important because governments often shape AI markets through what they buy, fund, approve or pilot. Strong procurement rules can create leverage over transparency, documentation, auditability, interoperability, security and vendor lock-in.

Indicator	Score = 0 Not present	Score = 1 Partially present	Score = 2 Fully present	Score
1. AI innovation ecosystem	No AI-focused innovation programmes, startup support, funding mechanisms or innovation hubs exist.	Some AI innovation initiatives exist but are limited, fragmented or not linked to policy priorities.	AI innovation programmes, startup support, funding mechanisms or innovation hubs are operational and aligned with public policy objectives.	
2. Regulatory sandboxes and pilots	No AI-related sandboxes, pilots or testbeds exist.	Isolated pilots or sandboxes exist but are not systematically evaluated or scaled.	AI-related sandboxes, pilots or testbeds operate in priority sectors as shared, regional resources to pool scarce capacity and generate lessons for policy or regulation.	
3. Regulatory learning and adaptation	Regulators do not participate in innovation or experimentation initiatives.	Regulators observe innovation initiatives but have limited influence on design, safeguards or learning.	Regulators actively participate in sandboxes and pilots as learning partners, and use lessons to inform guidance or regulatory reform.	
4. Competition and consumer protection readiness	AI-related competition and consumer risks are not recognized or addressed.	Authorities have acknowledged AI-related risks, such as algorithmic collusion, dark patterns, misleading claims or deceptive AI content.	Competition and consumer authorities issue AI-related guidance, warnings, investigations, enforcement actions or market studies.	
5. AI procurement frameworks	AI systems are procured like generic IT, with no AI-specific requirements.	Some procurement templates include AI-relevant provisions, but no standardized framework exists.	AI-specific procurement guidance, templates or procedures are in place, especially for high-risk AI systems.	

(continued)

Indicator	Score = 0 Not present	Score = 1 Partially present	Score = 2 Fully present	Score
6. Vendor accountability and risk management	Contracts do not address transparency, documentation, audit rights, interoperability, security or exit risks.	Some AI-related contract safeguards are included but are inconsistent or incomplete.	Procurement contracts systematically include AI-specific clauses on transparency, documentation, logs, audit rights, interoperability, security, performance and exit safeguards.	
7. Strategic innovation governance	Innovation, procurement and governance are disconnected.	Some alignment exists, but innovation programmes and procurement do not consistently support responsible AI objectives.	Innovation, procurement and regulatory objectives are strategically aligned to promote trustworthy, competitive and accountable AI markets.	

Maturity levels

Dimension score	Level	Description
0-3	(Level 1) Nascent	General innovation and procurement rules apply; AI is procured like generic IT; no AI-specific innovation or market oversight mechanisms exist.
4-7	(Level 2) Emerging	Isolated AI pilots, sandboxes or procurement adaptations exist, but regulators mostly observe and standardized safeguards are limited.
8-11	(Level 3) Established	Responsible AI innovation programmes are coordinated; regulators learn from sandboxes; procurement templates include AI-specific governance clauses, especially in high-risk domains.
12-14	(Level 4) Advanced	Innovation and procurement are strategically used to shape AI markets towards trustworthy solutions; governance criteria are embedded across procurement, funding, competition and consumer protection activities.

4.7 Dimension 7: Ethics, trust and societal preparedness

This dimension assesses whether ethical principles, rights safeguards, public trust mechanisms, transparency tools and redress channels are integrated into AI governance. Public trust is essential for sustainable AI adoption, particularly when AI systems affect access to services, rights, benefits, employment, credit, education, health, justice or public safety.

Indicator	Score = 0 Not present	Score = 1 Partially present	Score = 2 Fully present	Score
1. Ethical AI frameworks	No AI ethics principles, responsible AI guidance or equivalent framework has been adopted.	Ethics principles or guidelines exist but are not operationalized in law, procurement, regulation or procedures.	Ethical AI principles are formally adopted and operationalized through laws, regulations, procurement rules, internal procedures or sector-specific guidance.	
2. Rights and safeguards	Fairness, non-discrimination, transparency and human oversight are not reflected in governance frameworks.	Some safeguards are reflected in selected policies, guidelines or sectors.	Fairness, non-discrimination, transparency and human oversight are embedded in relevant laws, regulations, procurement rules or public-sector procedures.	
3. AI impact assessment frameworks	AI impact assessments, data protection impact assessments, regulatory impact assessments or human rights impact assessments are not used for AI systems.	Impact assessments are recommended or piloted for some systems but are inconsistent or not routinely implemented.	Impact assessments are required prior to AI rulemaking or are routinely implemented for high-risk AI systems.	
4. Transparency mechanisms	No public disclosures, algorithm registers or transparency tools exist for government use of AI.	Limited public disclosures or transparency pilots exist.	Public disclosures, AI system registers, algorithm registers or equivalent transparency tools are available and maintained.	
5. Accountability and redress	Individuals affected by AI-assisted decisions lack accessible general complaint, appeal or redress mechanisms.	General complaint channels exist but are not tailored to AI-assisted decisions.	Complaint, appeal, contestability, and redress mechanisms are accessible, understandable and applicable to AI-assisted decisions.	

(continued)

Indicator	Score = 0 Not present	Score = 1 Partially present	Score = 2 Fully present	Score
6. Public awareness and participation	There is no public communication, consultation or participation on AI governance.	Public communication or consultation occurs occasionally but is limited in reach or influence.	Public awareness, consultation, and participation mechanisms are regular, inclusive and reflected in policy or implementation.	
7. Trust monitoring and improvement	There is no monitoring of public trust, awareness or concerns about AI.	Some surveys, consultations or feedback mechanisms exist but are not systematically used.	Public trust and societal impacts are monitored, and findings inform policy updates, safeguards or public communication.	

Maturity Levels

Dimension score	Level	Description
0-3	(Level 1) Nascent	Ethical principles may be discussed but are not codified or operationalized; assessments, transparency and redress are limited or absent.
4-7	(Level 2) Emerging	Ethics statements or guidelines exist; some assessments and transparency measures are being piloted; redress channels are generic rather than AI-specific.
8-11	(Level 3) Established	Ethics and rights safeguards are embedded in laws, regulations or procedures; impact assessments are routine for high-risk systems; transparency and redress mechanisms are documented.
12-14	(Level 4) Advanced	Ethics and trust mechanisms are mature, participatory, transparent and continuously improved; public trust is monitored and informs governance adjustments.

4.8 Dimension 8: Implementation, supervision and enforcement preparedness

This dimension assesses whether regulators and competent authorities can enforce AI-related obligations and supervise AI systems over time. AI governance is only credible if institutions can investigate harms, request documentation, audit systems, receive complaints, impose corrective measures, coordinate across regulators and adjust supervision as technologies evolve.

Indicator	Score = 0 Not present	Score = 1 Partially present	Score = 2 Fully present	Score
1. Regulatory powers and mandates	Regulators lack authority to investigate AI-related risks, harms or compliance issues.	Regulators have general powers that may apply to AI, but mandates are implicit or unclear.	Relevant regulators have explicit or clearly applicable powers to investigate AI-related issues in their domains.	
2. Information access and corrective powers	Regulators cannot request AI documentation, records, logs or impose corrective measures.	Regulators can request some information or impose general measures, but powers are not adapted to AI systems.	Regulators can request documentation, records, logs, explanations and impose corrective measures or sanctions where appropriate.	
3. Supervisory infrastructure	No AI supervision units, focal points, task forces or dedicated oversight arrangements exist.	Some institutions have focal points or informal teams responsible for AI oversight.	Specialized AI supervision units, task forces, focal points or dedicated institutional arrangements exist.	
4. Audit and testing capacity	No AI-adapted supervision methods, audit frameworks, testing tools or technical assessment capabilities exist.	Some regulators are experimenting with audits, testing or assurance tools, but capability remains limited.	Regulators use or develop AI audit frameworks, test protocols, assurance tools or technical assessment methods.	
5. Enforcement practice	No AI-related guidance, investigations, supervisory reviews, enforcement actions or corrective measures exist.	Some guidance, thematic reviews or AI-related cases have been handled using adapted traditional tools.	Regulators regularly issue guidance, conduct AI-related investigations or reviews, and take corrective or enforcement action where needed.	
6. Complaint and incident management	No system exists for receiving, tracking, escalating or responding to AI-related complaints or incidents.	General complaint or incident channels can be used for AI issues, but tracking and escalation are limited.	AI-related complaints and incidents are received, tracked, escalated, investigated and resolved through defined procedures.	

(continued)

Indicator	Score = 0 Not present	Score = 1 Partially present	Score = 2 Fully present	Score
7. Cooperation and continuous improvement	Authorities do not participate in domestic or international AI enforcement cooperation and do not evaluate AI rules.	Domestic or international cooperation exists, to a certain extent, but it is irregular or not linked to supervisory practice.	Authorities participate in domestic coordination and international enforcement networks, and periodically evaluate and update AI-related rules, guidance and supervision methods.	

Maturity levels

Dimension score	Level	Description
0-3	(Level 1) Nascent	AI-related enforcement is minimal and ad hoc; regulators treat AI cases as generic without specific methods, tools, focal points or strategies.
4-7	(Level 2) Emerging	Some AI-related guidance, thematic reviews, or initial cases exist; internal awareness is growing; regulators are beginning to experiment with audits or adapted oversight tools.
8-11	(Level 3) Established	Systematic risk-based supervision of AI systems exists in several sectors; regulators issue regular guidance, cooperate across institutions and use or develop audit and testing tools.
12-14	(Level 4) Advanced	AI supervision is proactive, technology-enabled, and embedded in mainstream regulatory practice; enforcement records are robust; there is international cooperation and periodic rule evaluation.

4.9 Overall preparedness

The overall preparedness and scorecard results will be calculated based on the score achieved for each dimension, the corresponding percentage achieved and the associated maturity level.

Preparedness dimension	Score achieved	Maximum score	Maturity level (1 to 4)
1. Vision and strategic alignment		14	
2. Governance and institutional preparedness		14	
3. Digital and computing infrastructure		14	
4. Data governance and data ecosystems		14	
5. Talent, skills and institutional capabilities		14	

(continued)

Preparedness dimension	Score achieved	Maximum score	Maturity level (1 to 4)
6. Innovation and procurement preparedness		14	
7. Ethics, trust and societal preparedness		14	
8. Implementation, supervision and enforcement preparedness		14	
Total		112	

Overall score	Overall preparedness level
0-28	(Level 1) Nascent
29-56	(Level 2) Emerging
57-84	(Level 3) Established
85-112	(Level 4) Advanced

5 Conclusion: Collaborative frameworks and preparedness diagnostics as twin pillars of AI governance

The central message of this guide is that effective AI governance requires two mutually reinforcing pillars: **collaborative frameworks** and **preparedness diagnostics**. Collaborative frameworks address the institutional question: who needs to work together to govern AI across data protection, telecommunications, cybersecurity, competition, consumer protection, public procurement, sector regulation, human rights and innovation policy? Preparedness diagnostics address the implementation question: are those institutions ready to fulfil their respective roles, with the necessary mandates, tools, data access, technical skills, infrastructure, budget and enforcement capacity?

This distinction matters because many countries are now moving rapidly from AI principles and strategies towards binding laws, regulatory guidance, sector pilots, sandboxes and public sector deployment. The EU AI Act provides the most developed example of a comprehensive risk-based legal framework, but its implementation still depends on national authorities, market surveillance bodies, sector regulators, notified bodies, fundamental rights institutions and coordination mechanisms. Similar implementation challenges arise in different forms in Brazil, Bangladesh, Rwanda, Singapore, Germany, Spain and other jurisdictions. AI governance is thus no longer only about adopting the right policy language. It also requires building the institutional capacity to translate that language into practice.

The preparedness diagnostic in this guide (refer to sections 3 and 4) should therefore serve as a bridge between the collaborative AI framework and the preparedness diagnostic. The collaborative framework identifies the relevant institutions, coordination channels and

stakeholder groups, while the diagnostic assesses whether each component of the framework is functional. For example, if the collaborative framework includes a data protection authority, telecommunications regulator, competition authority, procurement body and health ministry, the diagnostic assesses whether those bodies have clear mandates, meet regularly, share information, issue joint guidance, understand high-risk AI use cases, and have the technical capacity to supervise them. For ease of reference, the AI collaborative framework roadmap is included as Annex 2.

This guide adopts a simple, three-step approach. First, policy-makers should use the **collaborative framework roadmap** to map the AI governance ecosystem: institutions, mandates, coordination bodies, sector regulators, advisory mechanisms and stakeholder participation. Second, they should use the **preparedness diagnostic** to assess whether the ecosystem can effectively operate across the eight dimensions: vision and strategic alignment; governance and institutional preparedness; digital and computing infrastructure; data governance; talent and institutional capabilities; innovation and procurement; ethics, trust and societal preparedness; and implementation, supervision and enforcement. Third, they should combine the results into a sequenced roadmap that identifies quick wins, medium-term reforms and longer-term capacity investments.

This combined approach helps to avoid two common implementation challenges. The first is the “paper framework” problem, where a country establishes an AI council, strategy or law but lacks the institutional capacity, data systems, procurement rules and supervisory tools to implement it. The second is the “technical pilot” problem, where AI systems are deployed in health, education, agriculture, finance, taxation, or public administration without sufficient legal safeguards, institutional coordination, transparency or redress mechanisms. Linking collaborative frameworks with preparedness diagnostics helps governments to address both gaps, enabling them to support innovation while ensuring that AI deployment is lawful, safe, rights-respecting, inclusive and institutionally sustainable.

For policy-makers and regulators, the practical value of this approach is clear. A combined framework and diagnostic can help to determine whether a country is ready to adopt AI legislation, whether existing regulators require additional powers, whether sandboxes should be established, whether public procurement templates need AI-specific provisions, whether a public-sector algorithm register is feasible, whether high-risk AI systems should be subject to additional safeguards prior to deployment, and where donor, public or private investment should be directed. It can also help governments to communicate transparently with citizens and industry about what AI can do, what safeguards are in place, where gaps remain and what steps will be taken next.

Ultimately, AI preparedness is not a one-time assessment but an ongoing governance practice. AI systems, risks, standards, markets and public expectations will continue to evolve. The diagnostic should be repeated periodically, updated as laws and technologies change, and linked to monitoring indicators, institutional workplans and budget decisions. Used in this way, the diagnostic becomes more than a measurement tool. It becomes a living instrument for collaborative AI frameworks: one that helps countries move from ambition to implementation, from fragmented oversight to coordinated action, and from isolated pilots to trustworthy, inclusive and accountable AI ecosystems.

Annex I: Illustrative application of the AI preparedness diagnostic: the case of Novara

A. Purpose of the annex

This annex provides an illustrative example of how the AI preparedness diagnostic can be applied in practice. The country example is fictional and is intended only to demonstrate how assessors can use the eight preparedness dimensions, indicator scoring tables, evidence review, and maturity levels to produce structured diagnostic findings.

The fictional country, Novara, is a lower-middle-income country, with a population of approximately 18 million, that is digitalizing its economy. It has made significant progress in broadband expansion, digital government, open data and innovation policy; however, its AI governance arrangements remain underdeveloped. Several ministries and regulators have begun experimenting with AI in public service delivery, agriculture, customs, tax administration and health, but institutional coordination, regulatory oversight, procurement safeguards and enforcement tools remain uneven.

The diagnostic was conducted using document review, institutional self-assessment and interviews with ministries, regulators, academic institutions, civil society, private-sector representatives and development partners. Each of the eight dimensions was assessed using seven indicators. Each indicator was scored from 0 to 2, where 0 means not present, 1 means partially present and 2 means fully present.

B. Summary of findings

Novara demonstrates emerging to established AI preparedness. It has a draft national AI strategy, a growing digital infrastructure base, a modern data protection law and several AI pilots in agriculture, health and public administration. However, its AI governance ecosystem remains fragmented. Coordination remains informal, public-sector AI capacity is limited, procurement rules do not yet include AI-specific safeguards, and regulators lack mature audit, testing and enforcement capabilities.

Overall, Novara scores 61 out of 112, corresponding to an overall maturity classification of Level 3 – established, although several foundational weaknesses remain.

C. Overall scorecard

Preparedness dimension	Score achieved	Maximum score	Maturity level
1. Vision and strategic alignment	9	14	Level 3 – established
2. Governance and institutional preparedness	7	14	Level 2 – emerging
3. Digital and computing infrastructure	10	14	Level 3 – established
4. Data governance and data ecosystems	8	14	Level 3 – established

(continued)

Preparedness dimension	Score achieved	Maximum score	Maturity level
5. Talent, skills and institutional capabilities	6	14	Level 2 – emerging
6. Innovation and procurement preparedness	8	14	Level 3 – established
7. Ethics, trust and societal preparedness	7	14	Level 2 – emerging
8. Implementation, supervision and enforcement preparedness	6	14	Level 2 – emerging
Total	61	112	Level 3 – established

D. How the score was calculated

Each dimension contains seven indicators. Each indicator is scored as follows:

Score	Meaning	Description
0	Not present	No meaningful evidence exists, or the activity is informal, isolated or absent.
1	Partially present	The indicator exists in draft, pilot, limited, fragmented or under-resourced form.
2	Fully present	The indicator is formally established, operational, adequately resourced and supported by evidence of implementation.

Each dimension has a maximum score of 14 points:

$$7 \text{ indicators} \times 2 \text{ points} = 14 \text{ points}$$

The overall preparedness score is calculated by adding the scores across all eight dimensions:

$$8 \text{ dimensions} \times 14 \text{ points} = 112 \text{ points}$$

For Novara: total = 61 points

This places Novara in the Level 3 – **established** range overall. However, the scorecard also shows important differences between dimensions. Novara performs relatively well on infrastructure and strategic alignment, but its performance is weaker on skills, governance coordination, ethics and enforcement.

E. Dimension-level assessment

1. Vision and strategic alignment

Novara has made substantial progress in establishing AI as a national policy priority. The government has prepared a draft national AI strategy and has already included AI-related

objectives in the Digital Transformation Strategy 2030 and the National Innovation Plan. However, the strategy is yet to be formally adopted, funding is incomplete and monitoring arrangements remain limited.

Indicator	Score	Rationale
AI strategy framework	1	A draft national AI strategy exists but has not yet been formally adopted.
Strategic integration	2	AI objectives have been included in the Digital Transformation Strategy and several sectoral strategies.
Opportunity and risk coverage	1	The draft strategy emphasizes productivity, innovation and public services, but risk safeguards are less developed.
Institutional ownership	2	The Ministry of Digital Transformation has been designated as lead, with roles for the telecommunications regulator and innovation agency.
Implementation readiness	1	A draft roadmap exists but lacks detailed sequencing and milestones.
Resource commitment	1	Some donor and innovation funding has been identified, but no dedicated national AI budget exists.
Monitoring and reporting	1	Basic monitoring indicators have been proposed but are not yet operational.
Total	9/14	Level 3 - established

Key finding: Novara has moved beyond general AI ambition, but strategy implementation is still vulnerable because adoption, funding and monitoring mechanisms remain incomplete.

2. Governance and institutional preparedness for collaborative AI frameworks

AI governance in Novara remains fragmented. Several institutions are active on AI-related issues, including the Ministry of Digital Transformation, the telecommunications regulator, the data protection authority, the competition authority and the cybersecurity agency. However, coordination remains informal and does not yet produce regular joint guidance or decisions.

Indicator	Score	Rationale
AI coordination structures	1	An informal AI task force exists but has no legal mandate or permanent secretariat.
Institutional mandates	1	Mandates have been partly defined, but overlaps exist between digital, data protection and sector regulators.
Inter-agency coordination	1	Inter-agency meetings take place but have not been institutionalized through formal procedures.
Operational collaboration	1	Some joint discussions have taken place, but have produced few documented outputs.
Regulatory cooperation	1	Regulators cooperate occasionally on data protection and cybersecurity issues.

(continued)

Indicator	Score	Rationale
Stakeholder engagement	1	Consultations are held with academia and industry, but civil society engagement is limited.
International cooperation	1	Novara participates in regional digital economy dialogues, but with limited AI-specific engagement.
Total	7/14	Level 2 - emerging

Key finding: Novara needs to formalize its AI coordination mechanism, clarify institutional mandates and create regular channels for joint guidance, stakeholder engagement and regulatory cooperation.

3. Digital and computing infrastructure

Novara has relatively strong digital infrastructure compared with peer countries. Broadband access has expanded rapidly, and most central government agencies use secure cloud services. However, some rural connectivity gaps remain, data centre capacity is concentrated in the capital, and access to AI compute remains limited outside universities and a small number of agencies.

Indicator	Score	Rationale
Connectivity readiness	2	Broadband and mobile coverage are broad, although some rural gaps remain.
Cloud readiness	2	A government cloud policy exists and several ministries use secure cloud services.
Data centre ecosystem	1	Data centres exist, but are concentrated in the capital and certification is uneven.
Compute capacity	1	Universities and selected ministries have limited GPU access, and no national AI compute programme exists.
Public sector infrastructure	2	Core digital public infrastructure supports digital ID, payments and e-services.
Resilience and energy reliability	1	Backup arrangements exist for priority systems, but outages still affect some public services.
Infrastructure strategy	1	Infrastructure planning mentions AI but does not yet address HPC, edge computing or AI energy needs in detail.
Total	10/14	Level 3 - established

Key finding: Novara has a solid infrastructure base for AI pilots and early deployment, but it needs a clearer compute strategy and stronger resilience planning.

4. Data governance and data ecosystems

Novara adopted the Data Protection Act three years ago and established a data protection authority. An open data portal exists and several ministries publish datasets. However, data

quality is inconsistent, data-sharing agreements are not standardized, and AI-related data protection guidance remains limited.

Indicator	Score	Rationale
Data protection framework	2	A modern data protection law is in force.
DPA capacity	1	The DPA is operational but under-resourced and has limited AI expertise.
Open data ecosystem	1	An open data portal exists, but many datasets lack meta-data and machine-readable formats.
Data-sharing governance	1	Data sharing occurs through ad hoc agreements rather than standardized frameworks.
Data quality and stewardship	1	Some agencies use data standards, but practices are inconsistent.
Privacy safeguards	1	Basic anonymization practices are used, but Privacy-enhancing technologies (PETs) and synthetic data are not common.
AI data readiness	1	Some AI-relevant datasets exist in agriculture, health and transport, but quality and access remain uneven.
Total	8/14	Level 3 – established

Key finding: Novara has the legal foundations for data governance, but implementation capacity, data quality, interoperability and AI-specific data safeguards need strengthening.

5. Talent, skills and institutional capabilities

Novara faces a significant public-sector skills gap. Universities produce AI and data science graduates, but government institutions struggle to recruit and retain technical staff. Most ministries rely on external vendors or donor-funded consultants for AI-related projects. The amount of training provided is increasing, but remains ad hoc.

Indicator	Score	Rationale
Public sector AI expertise	1	Some ministries have data specialists, but AI expertise is uneven.
Regulatory technical capacity	1	The telecommunications regulator has some technical staff, but most regulators lack AI expertise.
Institutional support mechanisms	1	A university-based AI centre provides ad hoc support, but no formal centre of excellence serves the government.
Professional development	1	AI training has been delivered to some officials but has not been institutionalized.
Academic and research partnerships	1	Several partnerships exist with universities, mostly project-based.

(continued)

Indicator	Score	Rationale
Applied knowledge ecosystem	1	External experts are used, but knowledge transfer to government is limited.
AI literacy and awareness	0	No broad AI literacy programme exists for public officials or citizens.
Total	6/14	Level 2 - emerging

Key finding: Skills constitute one of the most important bottlenecks for Novara. Without sustained training, fellowships and internal technical capacity, implementation and oversight will remain dependent on external actors.

6. Innovation and procurement preparedness

Novara has a growing AI innovation ecosystem. The national innovation agency funds AI pilots in agriculture, logistics and public administration. A fintech sandbox exists, and an AI health pilot is under development. However, procurement frameworks have not yet been updated to include AI-specific safeguards, and regulators are not systematically involved in sandbox learning.

Indicator	Score	Rationale
AI innovation ecosystem	2	AI innovation grants and startup support programmes are operational.
Regulatory sand-boxes and pilots	1	A fintech sandbox and several AI pilots exist, but coverage is limited.
Regulatory learning and adaptation	1	Regulators observe some pilots but are not consistently involved as learning partners.
Competition and consumer protection readiness	1	Authorities have acknowledged AI-related market risks but have not issued formal guidance.
AI procurement frameworks	1	Procurement guidance mentions digital systems but lacks AI-specific requirements.
Vendor accountability and risk management	1	Some contracts include security clauses, but auditability, logs, explainability and exit provisions are inconsistent.
Strategic innovation governance	1	Innovation and procurement are partially aligned, but responsible AI criteria are not yet embedded across funding programmes.
Total	8/14	Level 3 - established

Key finding: Novara has built momentum with respect to innovation, but public procurement must be strengthened to ensure that government-funded AI systems are transparent, auditable, secure, interoperable and accountable.

7. Ethics, trust and societal preparedness

Novara has adopted general digital ethics principles, and some agencies are beginning to discuss responsible AI. However, ethical principles have yet to be operationalized in procurement, regulation or sector guidance. AI impact assessments are not mandatory, and there is no public register of government AI systems.

Indicator	Score	Rationale
Ethical AI frameworks	1	General digital ethics principles exist but are not AI-specific or operationalized.
Rights and safeguards	1	Some transparency and non-discrimination safeguards exist in sector policies, but they are uneven.
AI impact assessment frameworks	1	A draft AI impact assessment template is being piloted in the health sector.
Transparency mechanisms	0	No public AI or algorithm register exists.
Accountability and redress	1	General complaint channels exist, but they are not tailored to AI-assisted decisions.
Public awareness and participation	1	Public consultations have been held on the draft AI strategy, but there is no systematic engagement with affected communities.
Trust monitoring and improvement	1	Limited public trust surveys have been conducted through donor-supported projects.
Total	7/14	Level 2 - emerging

Key finding: Novara should move from general ethical principles to operational safeguards, including AI impact assessments, public disclosure, algorithm registers and redress mechanisms for AI-assisted decisions.

8. Implementation, supervision and enforcement preparedness

Novara regulators are aware of AI-related risks but have limited tools to supervise AI systems. Existing laws give regulators general powers to investigate data protection, telecommunications, consumer protection and competition issues, but few of their powers explicitly refer to AI. There are no AI audit frameworks and, to date, no regulator has taken formal AI-related enforcement action.

Indicator	Score	Rationale
Regulatory powers and mandates	1	Regulators have general legal powers that may apply to AI, but mandates are not explicit.
Information access and corrective powers	1	Regulators can request some information, but access to logs, model documentation and training data is unclear.
Supervisory infrastructure	1	The DPA and telecom regulator have AI focal points, but no dedicated AI supervision units exist.

(continued)

Indicator	Score	Rationale
Audit and testing capacity	0	No AI audit or testing methodology is currently in use.
Enforcement practice	1	Some guidance on digital risks exists, but no AI-specific enforcement action has been taken.
Complaint and incident management	1	General complaint channels exist but do not classify or track AI-related complaints.
Cooperation and continuous improvement	1	Regulators participate in regional regulatory networks but not in specialized AI enforcement cooperation.
Total	6/14	Level 2 - emerging

Key finding: Novara AI governance credibility will depend on strengthening supervisory mandates, information access powers, audit tools, complaint handling mechanisms and cross-regulator enforcement cooperation.

F. Consolidated maturity profile

Dimension	Maturity level	Main strength	Main gap
Vision and strategic alignment	(Level 3) established	Draft strategy and integration into digital plans	Strategy not yet formally adopted or fully funded
Governance and institutional preparedness	(Level 2) emerging	Informal task force exists	Weak mandate and limited joint outputs
Digital and computing infrastructure	(Level 3) established	Strong cloud and digital public infrastructure	Limited AI compute and resilience planning
Data governance and data ecosystems	(Level 3) established	Data protection law and open data portal	Weak DPA capacity and inconsistent data quality
Talent, skills and institutional capabilities	(Level 2) emerging	University expertise exists	Public-sector AI skills gap
Innovation and procurement preparedness	(Level 3) established	Innovation grants and AI pilots	Procurement lacks AI-specific safeguards
Ethics, trust and societal preparedness	(Level 2) emerging	Initial ethics principles and consultations	No algorithm register or mandatory impact assessments
Implementation, supervision and enforcement	(Level 2) emerging	Regulators recognize AI as an emerging issue	No audit tools or enforcement practice

G. Priority recommendations for Novara

Based on the diagnostic findings and the consolidated maturity profile, Novara should prioritize reforms that convert early AI ambition into operational governance capacity. The sequencing

of the recommendations reflects both the country's relative strengths and its most urgent gaps. Novara already has established foundations in strategic alignment, digital infrastructure, data governance and innovation, but remains weaker with respect to institutional coordination, public-sector skills, ethics and trust safeguards, as well as supervision and enforcement. For this reason, the short-term priorities should focus first on adopting the national AI strategy, creating a formal coordination mechanism and introducing basic procurement, impact assessment and regulatory focal point arrangements. These actions are necessary preconditions for later reforms. The medium-term priorities should then be to build institutional capacity, technical expertise, compute access, transparency mechanisms and audit guidance. The longer-term priorities should focus on institutionalizing mature oversight, expanding risk-based supervision, strengthening societal preparedness, deepening international cooperation and reassessing progress through a follow-up diagnostic.

Short-term priorities: 0–12 months

Priority action	Lead institution	Rationale
Adopt the national AI strategy and publish an implementation roadmap	Ministry of Digital Transformation	Provides formal policy direction and implementation clarity
Establish a formal AI coordination council	Cabinet / Prime Minister's Office	Strengthens inter-agency coordination and accountability
Develop AI procurement guidance and standard contract clauses	Public Procurement Authority	Ensures transparency, auditability, security and vendor accountability
Pilot an AI impact assessment template in high-risk sectors	Ministry of Digital Transformation, DPA, sector regulators	Operationalizes ethics and risk management
Designate AI focal points in key regulators	DPA, telecommunications regulator, competition authority, consumer authority	Creates minimum supervisory capacity

Medium-term priorities: 12–24 months

Priority action	Lead institution	Rationale
Create an AI governance training programme for public officials and regulators	Civil Service Academy	Builds institutional capacity
Establish a government AI advisory panel or centre of excellence	Ministry of Digital Transformation / universities	Provides structured technical expertise
Develop a national AI compute access plan	Ministry of ICT / Research Ministry	Addresses compute bottlenecks
Create a public register of government AI systems	Ministry of Digital Transformation	Strengthens transparency and public trust

(continued)

Priority action	Lead institution	Rationale
Develop AI audit and testing guidance for regulators	DPA, telecommunications regulator, cybersecurity agency	Builds supervisory capability

Longer-term priorities: 24-36 months

Priority action	Lead institution	Rationale
Establish dedicated AI supervision units in major regulators	DPA, telecommunications regulator, competition authority	Institutionalizes AI oversight
Introduce risk-based AI supervision in priority sectors	Sector regulators	Aligns oversight with high-risk deployments
Expand AI literacy programmes for citizens and public officials	Education Ministry / Civil Service Academy	Builds societal preparedness
Strengthen cross-border cooperation on AI governance	Foreign Ministry / regulators	Supports alignment with international standards
Perform a follow-up diagnostic	AI Coordination Council	Measures progress and updates the roadmap

H. Illustrative conclusion

The diagnostic shows that Novara is no longer at a purely nascent stage of AI preparedness. It has important strategic, digital infrastructure, data governance and innovation foundations. However, the country's ability to govern AI responsibly will depend on whether it can formalize coordination, strengthen institutional capacity, operationalize ethics, modernize procurement, and build credible supervision and enforcement capabilities.

The immediate challenge Novara is facing is therefore not simply to adopt more AI pilots, but to ensure that AI deployment is supported by institutions, safeguards, skills and accountability mechanisms. The diagnostic provides a practical roadmap for moving from emerging AI activity to a more mature, coordinated and trustworthy AI governance ecosystem.

Annex II: From vision to implementation – a practical roadmap for national AI collaborative governance

Annex II aims to translate the diagnostic approach into a practical implementation pathway. While the main text explains the rationale for collaborative AI frameworks and the preparedness diagnostic tool, and Annex I illustrates how the tool can be applied in practice, Annex II shows how countries can move from assessment to action. It provides a sequenced roadmap for national AI collaborative governance, helping policy-makers and regulators to identify next steps, prioritize reforms, strengthen institutional coordination, build capacity, develop oversight tools and move from an AI vision and strategy towards credible implementation. This Annex was developed as part of: [A guide towards collaborative AI frameworks, published on the Digital Regulation Platform](#).

1. Foundational readiness: Awareness and visioning

Objective: Develop a national understanding of the relevance of AI, and set out a common vision.

Activities:

- ✓ Organize high-level awareness-raising workshops for cabinet members, parliamentarians and senior ministry officials to foster a common understanding of opportunities and risks associated with AI.
- ✓ Launch inclusive public education campaigns in partnership with civil society, youth networks and local governments to demystify AI and build public trust.
- ✓ Conduct a national SWOT (strengths, weaknesses, opportunities, threats) analysis to identify the country's unique position in the global AI landscape, paying special attention to data availability, infrastructure and human capital.
- ✓ Set out a national AI vision grounded in sustainable development, inclusive innovation and digital sovereignty.
- ✓ Convene inter-ministerial dialogues to align AI vision with sectoral plans (e.g., health, finance, justice, education, public services).
- ✓ Identify and integrate cross-cutting priorities (e.g., gender equality, green economy, digital trade and digital public services).
- ✓ Commission foresight studies on the long-term implications of AI for the domestic labour market, social cohesion and governance.

Outcomes: National AI vision adopted; baseline awareness among political and institutional leaders, and clear understanding developed of national strengths and weaknesses.

2. Building the Architecture: Stakeholder mapping and coordination

Objective: Identify institutional actors and establish mechanisms for collaboration and coordination.

Activities:

- ✓ Map relevant AI stakeholders across the public sector (e.g., digital ministries, telecommunications regulators, national statistical offices, data protection offices), private sector, academia and civil society.
- ✓ Conduct mandate mapping to clarify overlaps and gaps among government entities (e.g., Ministry of Science vs Ministry of Justice).
- ✓ Establish or strengthen a national AI coordination body (e.g., AI task force, national AI steering committee inter-ministerial task force), with a clear mandate for strategy oversight and implementation.
- ✓ Create a multistakeholder advisory platform (such as an AI ethics forum or civil society AI roundtable) to ensure that diverse perspectives inform policy.
- ✓ Institutionalize regular cross-sectoral coordination platforms to facilitate joint strategy development and coherent implementation.
- ✓ Engage with international partners (e.g., ITU, UNESCO and UNDP) for technical support and alignment with global standards.

Outcomes: Stakeholder ecosystem clarified; inclusive and coordinated governance architecture established.

3. Assessing the landscape: Institutional readiness and legal gap assessment

Objective: Evaluate legal, institutional and technical environments to identify governance gaps.

Activities:

- ✓ Conduct AI preparedness assessments using international tools (e.g., Stanford AI Index Report, The Global Index on Responsible AI (GIRAI), AI Readiness Index – Oxford Insights) to benchmark national capabilities.
- ✓ Review existing national laws and frameworks (systematic frameworks such as the OECD mapping tool) that impact AI (including data protection, e-governance, cybersecurity, consumer rights, competition, intellectual property (IP), privacy and non-discrimination).
- ✓ Identify gaps in legal coverage of AI-specific risks (such as algorithmic bias, explainability and liability).
- ✓ Assess inter-agency capacities for AI oversight (staffing, skills, budget and ICT infrastructure).
- ✓ In collaboration with sectoral regulators, conduct high-risk sectoral case studies (e.g., facial recognition in law enforcement, predictive tools in welfare, AI in credit scoring) to understand context-specific challenges.

Outcomes: Baseline legal-institutional landscape mapped; regulatory and institutional priorities relating to AI identified.

4. Designing the framework: Strategy and legislation

Objective: Draft a national AI governance strategy and legal framework aligned with international norms and standards.

Activities:

- ✓ Co-develop a national strategy grounded in principles such as ethics, safety, accountability and human rights. This strategy should include distinct pillars, such as Governance, Technology and R&D, Data, Infrastructure, Ecosystem and Talent.
- ✓ Align policy frameworks with guidance from international organizations (e.g., ITU, UNESCO Recommendation on AI Ethics, OECD Principles on AI and Global Partnership on Artificial Intelligence (GPAI)).
- ✓ Include dedicated sections on algorithmic transparency and accountability, cybersecurity, data governance, funding/innovation incentives, and the provision of public services and access to justice.
- ✓ Embed co-regulatory innovative and agile instruments (such as impact assessments, sandboxes and certification schemes).
- ✓ Draft enabling or reinforcing legislation in collaboration with legal and technical experts.
- ✓ Ensure meaningful participation of ministries, agencies, parliamentarians and civil society.
- ✓ Draft complementary legislation, if necessary, to enable or enforce the AI governance framework.

Outcomes: AI governance strategy drafted and validated; legal tools prepared for operationalization.

5. Empowering institutions: Institutional design and capacity building

Objective: Strengthen or establish dedicated institutions and build public sector capacities for oversight.

Activities:

- ✓ Establish a lead AI regulator or assign oversight roles to existing bodies (e.g., telecommunications/ICT regulator, data protection authority and judiciary).
- ✓ Clearly define mandates, powers and coordination roles across agencies.
- ✓ Set up sectoral oversight mechanisms (e.g., AI ethics review boards in health, education, finance).
- ✓ Deliver AI literacy and redress training for judges, ombudspersons and frontline officials.
- ✓ Partner with ITU Academy, innovation labs, and universities for national capacity development in AI governance.

Outcomes: Oversight architecture defined; capacity-building mechanisms institutionalized.

6. Activating governance: Policy instruments and enforcement tools

Objective: Equip government agencies with tools to enforce safe, ethical and rights-respecting AI use.

Activities:

- ✓ Develop AI procurement and deployment guidelines for line ministries.
- ✓ Require AI system deployers to conduct algorithmic and data protection impact assessments (mandate impact assessments for high-risk systems).
- ✓ Institutionalize AI model documentation (e.g., datasheets, model cards and audit trails).
- ✓ Pilot regulatory sandboxes and co-regulation labs to safely test high-risk AI systems in a controlled environment, with regulatory supervision.
- ✓ Explore "living legislation" mechanisms, where specific technical standards or risk classifications can be updated via secondary legislation based on monitoring data, without requiring a full parliamentary process.
- ✓ Introduce mechanisms for explanation, appeal and redress in automated decision-making.

Outcomes: AI governance toolkit established; accountability and safeguards embedded.

7. Ensuring adaptability: Monitoring, evaluation and iteration

Objective: Establish adaptive governance to track performance and learning from implementation, and adapt the strategy over time.

Activities:

- ✓ Define sector-specific key performance indicators for fairness, accuracy, accessibility and legal compliance.
- ✓ Institutionalize periodic inter-agency reviews of the AI strategy and legal framework every 2–3 years, involving industry, civil society and the academia, to ensure alignment with technological advancements.
- ✓ Publish audit results and public registers of government AI deployments.
- ✓ Use real-world feedback and ombudsperson reports to revise AI policy instruments.

Outcomes: Evidence-based AI governance cycle operationalized; public trust strengthened.

8. Looking ahead: Future-proofing and international collaboration

Objective: Prepare for emerging AI risks and opportunities, and actively shape global AI governance.

Activities:

- ✓ Establish a foresight unit or task force to monitor emerging models (e.g., AGI, Agentic AI).
- ✓ Join or establish international and regional AI alliances (e.g., ITU AI for Good, UNESCO AI Coalitions, Global Partnership on AI (GPAI)).
- ✓ Sign memorandum of understanding (MoU) for knowledge exchange with peer regulators and research centres.
- ✓ Collaborate with international standards bodies (e.g., ITU, ISO, IEEE) on AI testing, certification and harmonization.
- ✓ Co-develop interoperable safety protocols, especially for high-risk and transboundary AI applications.

Outcomes: National AI governance framework aligned with global norms; international leadership role strengthened.

Source: ITU, [A guide towards collaborative AI frameworks](https://digitalregulation.org/a-guide-towards-collaborative-ai-frameworks/), ITU World Bank Digital Regulation Platform, digitalregulation.org/a-guide-towards-collaborative-ai-frameworks/

Office of the Director
International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435

Office of the Deputy Director
Operations Coordination Department (DDR)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5131

**Digital Networks and Environment
Department (DNE)**

Email: bdt-dne@itu.int
Tel.: +41 22 730 5421

**Digital Knowledge Society
Department (DKS)**

Email: bdt-dks@itu.int
Tel.: +41 22 730 5900

**Projects, Partnerships and Digital
Skills Department (PPS)**

Email: bdt-pps@itu.int
Tel.: +41 22 730 5447

Africa

Ethiopia

**International Telecommunication
Union (ITU) Regional Office**
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopia

Email: itu-ro-africa@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroon

**Union internationale des
télécommunications (UIT)**
Bureau de zone
Immeuble CAMPOST, 3^e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Cameroon

Email: itu-yaounde@itu.int
Tel.: +237 22 22 9292
Tel.: +237 22 22 9291
Fax: +237 22 22 9297

Senegal

**Union internationale des
télécommunications (UIT)**
Bureau de zone
8, Route du Méridien Président
Immeuble Rokhaya, 3^e étage
Boîte postale 29471
Dakar - Yoff
Senegal

Email: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

Zimbabwe

**International Telecommunication
Union (ITU) Area Office**
USAF POTRAZ Building
877 Endeavour Crescent
Mount Pleasant Business Park
Harare
Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 242 369015
Tel.: +263 242 369016

Americas

Brazil

**União Internacional de
Telecomunicações (UIT)**
Escritório Regional
SAUS Quadra 6 Ed. Luis Eduardo
Magalhães,
Bloco "E", 10^o andar, Ala Sul
(Anatel)
CEP 70070-940 Brasília - DF
Brazil

Email: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados

**International Telecommunication
Union (ITU) Area Office**
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

Email: itubridgetown@itu.int
Tel.: +1 246 431 0343
Fax: +1 246 437 7403

Chile

**Unión Internacional de
Telecomunicaciones (UIT)**
Oficina de Representación de Área
Merced 753, Piso 4
Santiago de Chile
Chile

Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras

**Unión Internacional de
Telecomunicaciones (UIT)**
Oficina de Representación de Área
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cia
Apartado Postal 976
Tegucigalpa
Honduras

Email: itutegucigalpa@itu.int
Tel.: +504 2235 5470
Fax: +504 2235 5471

Arab States

Egypt

**International Telecommunication
Union (ITU) Regional Office**
Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypt

Email: itu-ro-arabstates@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia-Pacific

Thailand

**International Telecommunication
Union (ITU) Regional Office**
4th floor NBTC Region 1 Building
101 Chaengwattana Road
Laksi,
Bangkok 10210,
Thailand

Email: itu-ro-asiapacific@itu.int
Tel.: +66 2 575 0055

Indonesia

**International Telecommunication
Union (ITU) Area Office**
Gedung Sapta Pesona
13th floor
Jalan Medan Merdeka Barat No. 17
Jakarta 10110
Indonesia

Email: bdt-ao-jakarta@itu.int
Tel.: +62 21 380 2322

India

**International Telecommunication
Union (ITU) Area Office and Innovation
Centre**
C-DOT Campus
Mandi Road
Chhatarpur, Mehrauli
New Delhi 110030
India

Email: itu-ao-southasia@itu.int
Area Office: itu-ao-southasia@itu.int
Innovation
Centre: itu-ic-southasia@itu.int
Website: ITU Innovation Centre in
New Delhi, India

CIS

Russian Federation
**International Telecommunication
Union (ITU) Regional Office**
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation
Email: itu-ro-cis@itu.int
Tel.: +7 495 926 6070

Europe

Switzerland

**International Telecommunication
Union (ITU) Office for Europe**
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: euregion@itu.int
Tel.: +41 22 730 5467

International Telecommunication Union
Telecommunication Development Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN 978-92-61-43391-8



9 789261 433918

Published in Switzerland
Geneva, 2026

Adobe Stock