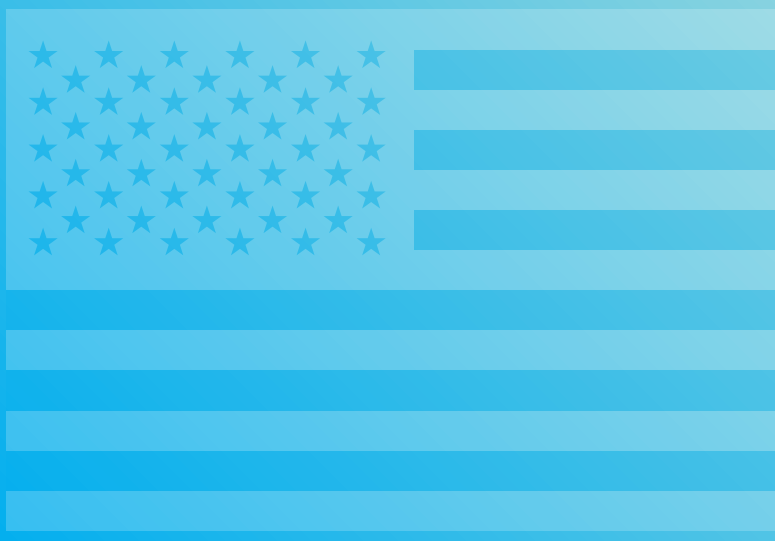
TechBetter

The EU AI Act Meets NIST AI RMF

A unified AI governance framework



Ravit Dotan techbetter.ai

Foreword

The EU AI Act and the NIST AI RMF are two of the most influential and comprehensive AI governance standards in the world. The EU AI Act is the flagship AI regulation in the European Union. It recently came into force and will gradually become binding over the next couple of years. The NIST AI Risk Management Framework (RMF) was created by the US government and it has gained popularity and traction in the US government and in the AI industry.

The TechBetter framework unifies these two powerful standards into a single, ready-to-use questionnaire. The framework can help organizations evaluate themselves or other organizations, such as vendors or portfolio companies.

Feel free to jump into the questionnaire itself and start evaluating!

If you'd like more support, we are offering individual consulting and workshops to organizations that develop, use, procure, invest, or engage with AI in other ways.

For more information and registration to our workshops, visit:
https://www.techbetter.ai/workshops

For more and to get in touch

For more information about the framework and additional case studies: https://www.techbetter.ai/rai-maturity-model

For support in implementing this process in your organization and for hosting similar competitions at your event, get in touch here: https://www.techbetter.ai/contact

Ravit Dotan,TechBetter
www.techbetter.ai
/ravit-dotan

Table of **Contents**

1

Introduction

About
The TechBetter Framework

What this framework is

The TechBetter framework is a tool for evaluating and improving AI governance. It is based on two influential standards: The NIST AI Risk Management Framework (AI RMF), the most influential US AI governance standard, and The EU AI Act, which is the flagship AI regulation of the European Union. The framework unifies the requirements in both standards and makes them accessible through a comprehensive and flexible questionnaire.

How this framework helps

The TechBetter framework is built to support multiple actors across the AI value chain. Organizations that develop or deploy AI-enabled tools can use the framework to evaluate their own governance at any stage of the development life cycle. Organizations that buy or invest in AI-enabled products can use it during due diligence and other stages of the procurement/investment process.

AI developers and users	AI bueyrs and investors
Use it to evaluate your own AI governance and improve it	Use it to evaluate prospective vendors and portfolio companies.

Workshops and consulting for support

Feel free to jump into the questionnaire itself and start evaluating!

If you'd like more support, we are offering individual consulting and workshops. Registration and additional information at: https://www.techbetter.ai/workshops

About The TechBetter Framework

The History of This Framework

The framework is based on academic research and practical experience. The work started as an academic research project that built an AI governance maturity model based on the NIST AI RMF and was later published as an IEEE technical report. That framework was implemented in two hackathons and piloted through public case studies. The TechBetter framework presented in this document adds the EU AI Act and lessons from the implementation.

We are thankful to those who contributed to and participated in the process:

Dr. Borhane Blili-Hamelin, Prof. Ravi Madhavan, Prof. Jeanna Matthews, Dr. Joshua Scarpino, Dr. Carol Anderson, Ric Mclaughlin, Benny Esparra, All Tech is Human, AI4Gov Masters Program, Light-it, Koko Home, and an anonymous tech company.

Additional Resources

All materials related to this framework are available at www.techbetter.ai/rai-maturity-model

The materials include the following:

- **IEEE report** - Presents the NIST-based version of the framework
- **Academic paper** - Presents the rationale and scholarship behind the framework
- **All Tech is Human hackathon report** - Presents case studies of using the framework to evaluate companies' AI governance externally, based on publicly available information
- **AI4Gov hackathon report** - Presents Case studies of using the framework to evaluate AI governance internally in early-stage projects
- **Light-It case study** - Reflections from a company that used the framework to self-evaluate

About
The NIST AI RMF

What is the NIST AI RMF?

The NIST AI Risk Management Framework (AI RMF) is one of the most influential AI governance guidelines. NIST is the US National Institute for Standards and Technology and is a part of the US Department of Commerce. While the RMF is not legally binding, many US initiatives rely on it. A prominent example is the most recent AI Executive Order, which directs government offices to incorporate the RMF into safety guidelines.

High Level Overview

The guidelines in the AI RMF are divided into the following four functions (p. 20 in the RMF):

- **MAP** - Context is recognized and risks relating to context are identified.
- **MEASURE** - Identified risks are assessed, analyzed, or tracked.
- **MANAGE** - Risks are prioritized and acted upon based on a projected impact.
- **GOVERN** - A culture of risk management is cultivated and present.

Each of these functions contains multiple categories and subcategories.

For example, the second MEASURE category is

- **MEASURE 2**: AI systems are evaluated for trustworthy characteristics.

And one of the subcategories in this category is

- **MEASURE 2.11**: Fairness and bias – as identified in the MAP function – are evaluated and results are documented.

The four NIST AI governance functions.
Image from NIST

About
The EU AI Act

What is the EU AI Act?

The EU AI Act is the flagship AI regulation of the European Union, putting in place obligations for AI systems and General Purpose models (GPAI). The Act recently passed into law and will be gradually coming into effect over the next couple of years. While the Act is only a law in the European Union, it applies beyond it. It is enough that one of the following holds:

Influence in scope (Article 2.1)			
The system affects people in the EU	The outputs will be used in the EU	The system is placed in the EU market	The deployer is in the EU

Who is subject to the Act?

The Act applies to many actors along the supply chain, including companies that develop AI and companies who deploy it, with most obligations to those who develop it.

Roles in scope (Article 3.2-8)

- **Provider** - Develops the AI/GPAI
- **Deployer** - Uses the AI/GPAI professionally
- **Importer** - EU-based and puts the tech into EU market under a non-EU party name
- **Distributer** - Makes the AI/GPAI available in the EU and isn't provider or importer
- **Authorized representative** - EU-based and represents a non-EU party
- **Product Manufacturer** - Puts AI on market with their product under their own name
- **Non-providers may count as providers** - E.g., if they make substantial changes or put the system under their name (Article 25)

About
The EU AI Act

Key Definitions

Artificial Intelligence (AI)

"a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments" (Article 3.1)

General Purpose AI model (GPAI)

"an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market" (Article 3.63)

General Purpose AI model (GPAI) with Systemic Risk

A GPAI that meets any of the following conditions:
"(a) it has high impact capabilities evaluated on the basis of appropriate technical tools and methodologies, including indicators and benchmarks;
(b) based on a decision of the Commission, ex officio or following a qualified alert from the scientific panel, it has capabilities or an impact equivalent to those set out in point (a) having regard to the criteria set out in Annex XIII." (Article 51)

High Risk AI System

An AI system is considered high risk if it included in the High Risk lists (article 6)

About
The EU AI Act

Three types of requirements

The Act assigns different obligations depending on the the context. In addition to variability by actor type already mentioned above, the main deciding factors are the use case, type of technology, and type of human interaction. The key requirements are as follows.

Use case	**Prohibited use cases,** List: Article 5	**Prohibited in the EU**
	High risk use cases, List: Article 6	**High risk obligations** Esp. Chapter III, Sections 2 +3
GPAI	**General Purpose AI model,** Def. Article 3.63	**Provider obligations**, Article 53
	GPAI with systemic risk, Def. Article 51	**Provider obligations**, Article 55
Special Transp-arency	**Generates content**, Def. Article 50.2	**Transparency obligations**, Article 50.2
	Generates deepfakes, Def. Article 50.4	**Transparency obligations**, Article 50.4
	Interacts with humans, Def. Article 50.1	**Transparency obligations**, Article 50.1
	Emotion recognition or biometric categorization, Def. Article 50.3	**Transparency obligations**, Article 50.3

About
The EU AI Act

Timeline

The Act entered into force on August 1, 2024 and is now in the process of gradually coming to effect over. The following are the key obligations in each milestone. For the full timeline, see Article 113 and the helpful summaries by the FFLI and IAPP.

Feb 5. 2025
Prohibited apps

Prohibited applications
Applications in the "unacceptable risk" category are prohibited
Article 5

AI literacy
AI providers and deployers must ensure AI literacy of their staff and operators
Article 4

Aug 2, 2025
GPAI & Penalties

GPAI models
Obligations for GPAI models apply
Articles 53, 55

Penalties
Penalties for non-compliance apply
Article 99

Feb 5, 2026
Almost all the Act comes into effect

High Risk Obligations
Apply to all high risk systems expect for AI in safety components in Article 6.1. The key obligations are in Chapter III, Sections 2 +3

Transparency Obligations
All transparency obligations apply
Article 50

Aug 2, 2027
All the Act is in effect

All High Risk Obligations
End of the exception for Article 6.1

2

High Level
Questionnaire Overview

High Level
What's in the questionnaire

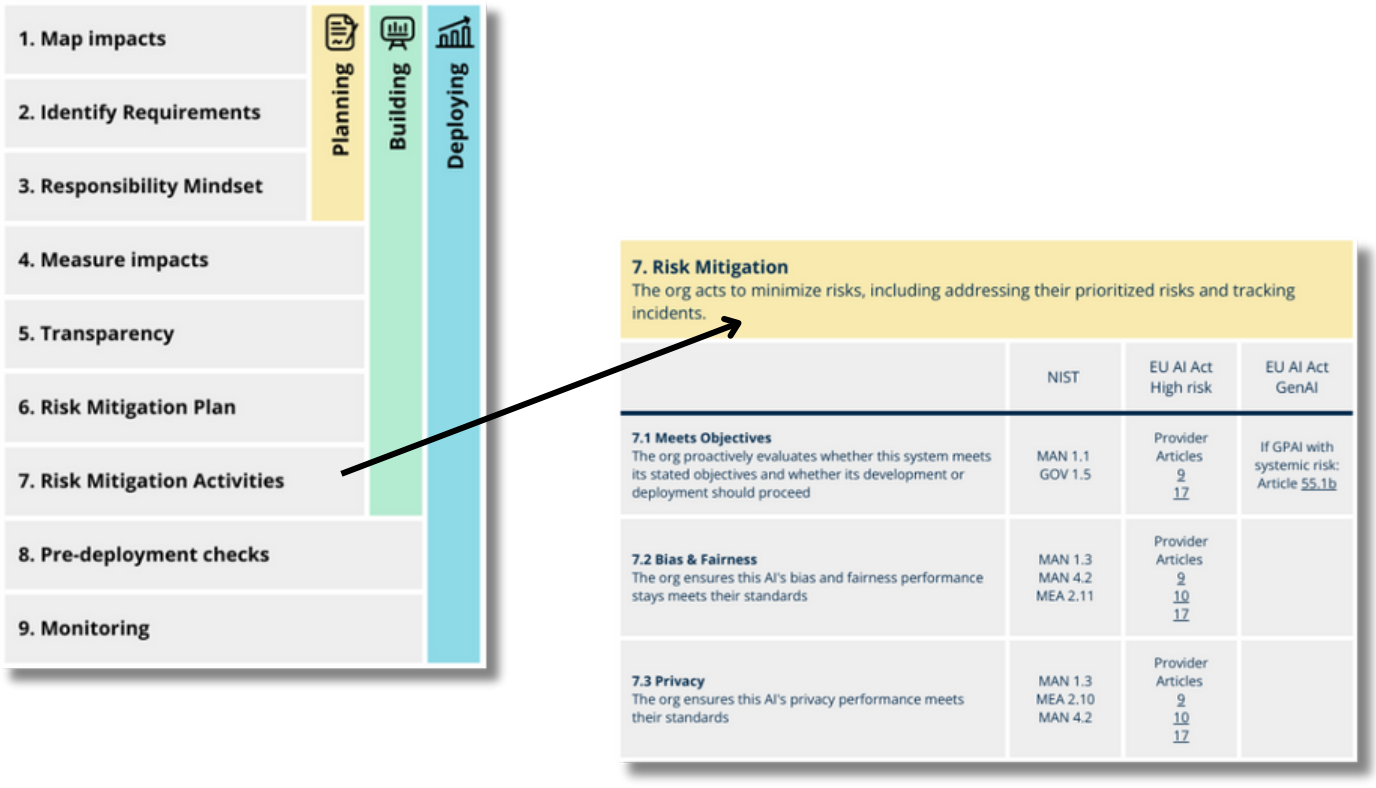
How the questionnaire is organized

The questionnaire is composed of a list of statements. Each of these statements represents content from the NIST AI RMF, EU Act, or both, and they are all about the organization's AI governance activities.

For example, one of the statements in the building stage is:

7.2 The org ensures this AI's bias and fairness performance stays meets their standards

The statements are divided into nine topics, and the topics are organized into three stages of the development life-cycle: planning, building, and deploying.



High Level
What's in the questionnaire

How to use the questionnaire

The questionnaire can be used in multiple ways, depending on your needs and context:

- **Granularity** - If you want a fine-grained evaluation should evaluate the organization on all the statements. However, if a shorter evaluation would be enough, you can evaluate the organization of the topics as a whole, brining the questionnaire down to nine questions.

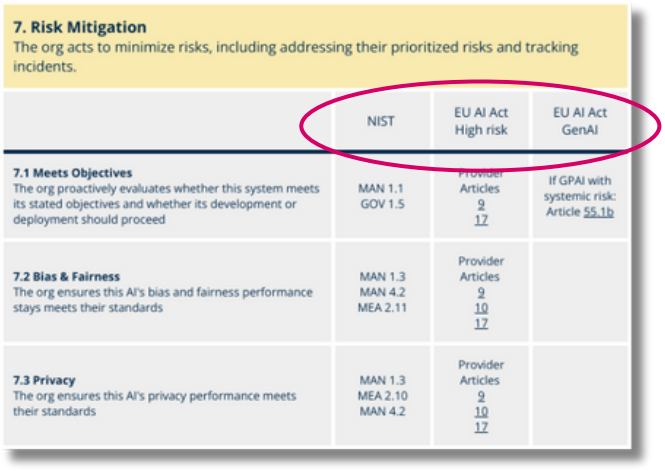
- **Life-cycle stage** - Some of the statements only become relevant in certain life-cycle stages. For example, statements about pre-deployment checks are only relevant pre-deployment. Therefore, you only need to use the statements relevant to the life-cycle stage the AI system or feature are in.

- **Multiple AI systems** - Organizations may have more than one AI system. For a fine-grain evaluation, it is best to evaluate each system separately. However, when a more high-level evaluation is needed, you can evaluate the organization as a whole.

Unifying the NIST AI RMF and the EU AI Act

The questionnaire unifies the NIST AI RMF and the EU AI Act through presenting a single list of statements for evaluation that represents content from both. You can see how in the three right-most columns:

- **NIST** - shows the relevant NIST items
- **EU AI High Risk** - shows the relevant articles that apply to High Risk systems
- **EU AI Act GenAI** - shows the relevant articles that relevant for GenAI: GPAI with or without systemic risk, and transparency obligations.



7. Risk Mitigation
The org acts to minimize risks, including addressing their prioritized risks and tracking incidents.

	NIST	EU AI Act High risk	EU AI Act GenAI
7.1 Meets Objectives The org proactively evaluates whether this system meets its stated objectives and whether its development or deployment should proceed	MAN 1.1 GOV 1.5	Provider Articles 9 17	If GPAI with systemic risk: Article 55.1b
7.2 Bias & Fairness The org ensures this AI's bias and fairness performance stays meets their standards	MAN 1.3 MAN 4.2 MEA 2.11	Provider Articles 9 10 17	
7.3 Privacy The org ensures this AI's privacy performance meets their standards	MAN 1.3 MEA 2.10 MAN 4.2	Provider Articles 9 10 17	

High Level
How the Framework Helps

Testimonials

Users of this framework in workshops, hackathons, and 1-1 engagements indicate that the evaluation process was helpful and important.

"The experience was eye-opening for me. It was very helpful to have a framework to work off of. I often think about the topics that the framework walks you through, but until working with it I did not have a robust way of assessing the topics and a way to ground and level my assessment. I found it very helpful"

-- Software Engineer

"I think that the [framework] raises many excellent questions that AI companies and projects should strive to address, and to do so in a requisitely comprehensive way. I value having the [framework] as a reference to return to as our project continues to develop, and as a tool to plan for future considerations"

-- Tech Strategist

"Auditors and regulatory bodies can utilize the questionnaire as a standardized tool for evaluating companies' AI governance practices. It provides a structured framework for assessing compliance with relevant regulations, standards, and ethical guidelines"

-- AI Ethicist

"The framework is a great sounding board for organisations at different phases of their AI journey. It enables them to catch issue[s] early in the system reducing cost and reputation implications"

-- Technology Consultant

3

Deep Dive
Full Questionnaire

Full Questionnaire

Questions for planning phases and on

1. Map Impacts

The org clearly defines what the AI is supposed to do and its impacts, including scope, goals, methods, and negative and positive potential impacts of these activities.

	NIST	EU AI Act High risk	EU AI Act GenAI
1.1 Goals The goals, scope, and methods of this AI system are well defined.	MAP 1.3 MAP 2.1 MAP 3.3		
1.2 Positive Impacts The benefits and potential positive impacts of this AI system, including the likelihood and magnitude, have been identified.	MAP 1.1 MAP 3.1 MAP 5.1 GOV 4.2		
1.3 Business Value The business value of this AI system has been identified.	MAP 1.4 MAP 3.1		
1.4 Negative Impacts The possible negative impacts of this AI system, including the likelihood and magnitude, have been identified.	MAP 5.1 GOV 4.2		
1.5 Costs of Malfunction The potential costs of malfunctions of this AI system, including non-monetary costs such as decreased trustworthiness, have been identified.	GOV 3.2		
1.6 Unexpected Impacts Processes to integrate input about unexpected impacts are implemented.	GOV 5.2		
1.7 Methods and Tools Methods and tools we use for mapping impacts have been identified.	MAP 2.3 MAP 4.1		
1.8 Input Diversity Diverse stakeholders inform the mapping process, including diverse skills and demographic backgrounds	MAP 1.2 GOV 3.1 GOV 5.1 GOV 5.2		

Full Questionnaire:

Questions for planning phases and on

2. Identify Requirements
The org identifies the requirements the AI must meet, including compliance, certifications, and human oversight needs.

	NIST	EU AI Act High risk	EU AI Act GenAI
2.1 Human Oversight Human oversight processes are identified.	GOV 3.2 MAP 3.5	Provider Article 14	
2.2 Standards Relevant technical standards and certifications have been identified.	MAP 1.6 MAP 3.4	Provider Article 17.1e	
2.3 Legal Relevant legal requirements have been identified.	GOV 1.1	Provider Article 17.1a	

Full Questionnaire:

Questions for planning phases and on

3. Mindset and Policies
The org facilitates a mindset of responsibility, for example, by providing AI ethics training to relevant personnel, clearly defining relevant roles, establishing policies, and implementing practices for critical thinking.

	NIST	EU AI Act High risk	EU AI Act GenAI
3.1 Policies Policies and guidelines about AI ethics are documented.	GOV 1.2 GOV 1.4	Provider Article 10	
3.2 Roles Roles, responsibilities, and lines of communication related to AI risk management are well-defined.	GOV 2.1	Provider Article 17.1m	
3.3 Training AI ethics training is provided to relevant personnel.	GOV 2.2	Provider & Deployer Articles 26.2 4	
3.4 Critical Thinking Practices to foster critical thinking about AI risks are implemented.	GOV 4.1		
3.5 Leadership Executive leadership takes responsibility for decisions related to AI risks.	GOV 2.3	Provider Article 17.1m	

Full Questionnaire:

Questions for building phases and on

4. Measuring Risk

The org tests this system and measure potential negative impacts.

	NIST	EU AI Act High risk	EU AI Act GenAI
4.1 Strategy The org periodically re-evaluates the strategy for measuring the impacts of this AI. It includes choosing which impacts we measure. It also includes how we will approach monitoring unexpected impacts and impacts that can't be captured with existing metrics.	MEA 1.1 MEA 3.1 MEA 3.2 MAP 2.3	Provider Articles 9 10 17 72	If GPAI with systemic risk Article 55
4.2 Methods The org has a clear set of methods and tools to use when measuring the impacts of this AI, including the metrics and datasets we use.	MEA 1.2 MEA 2.1 MEA 3.1 MEA 3.2 MAP 2.3	Provider Articles 9.7 17.1d 60	
4.3 Effectiveness The org evaluates the effectiveness of our measurement processes.	MEA 1.2 MEA 2.13		
4.4 Performance The org regularly evaluates the performance of this AI system in conditions similar to deployment.	MEA 2.3	Provider Articles 9 17	
4.5 Bias and Fairness The org regularly evaluates bias and fairness issues related to this AI.	MEA 2.11	Provider Articles 9 17	
4.6 Privacy The org regularly evaluates privacy issues related to this AI system.	MEA 2.10	Provider Articles 9 17	
4.7 Environmental The org regularly evaluates environmental impacts related to this AI.	MEA 2.12	Provider Articles 9 17	

Full Questionnaire:
Questions for building phases and on

4. Measuring Risk (Continued)
We test this system and measure potential negative impacts.

	NIST	EU AI Act High risk	EU AI Act GenAI
4.8 Transparency and accountability The org regularly evaluates transparency and accountability issues related to this AI system.	MEA 2.8	Provider Articles 9 17	
4.9 Security The org regularly evaluates security and resilience issues related to this AI.	MEA 2.7	Provider Articles 9 17	If GPAI with systemic risk: Article 55
4.10 Explainability The org regularly evaluates explainability issues related to this AI.	MEA 2.9	Provider Articles 9 17	
4.11 Third-party The org regularly evaluates third-party issues, such as IP infringement, related to this AI system.	MEA 1.1 GOV 6.1	Provider Articles 9 17	
4.12 Human oversight The org regularly evaluates human oversight issues related to this AI.	MEA 1.1 MAP 3.5 GOV 3.2	Provider Articles 9 17	
4.13 Safety The org regularly evaluates safety issues related to this AI.	MEA 2.6	Provider Articles 9 17	

Full Questionnaire:

Questions for building phases and on

4. Measuring Risk (Continued)

The org tests this system and measure potential negative impacts.

	NIST	EU AI Act High risk	EU AI Act GenAI
4.14 Other The org regularly evaluates other impacts related to this AI system	MEA 1.1	Provider Articles 9 17	
4.15 Human subjects If evaluations use human subjects, they are representative and meet appropriate requirements.	MEA 2.2 MEA 2.6	Articles 9.7 60	
4.16 Diverse input Consultations with diverse domain experts and end users inform measurement approaches, results, and progress.	MEA 1.3 MEA 3.3 MEA 4.1 MEA 4.2 MEA 4.3 GOV 5.2 GOV 3.1		

Full Questionnaire:

Questions for building phases and on

5. Transparency

The org documents information about the system, including explaining how it works, limitations, and risk controls.

	NIST	EU AI Act High risk	EU AI Act GenAI
5.1 Limitations and Oversight The org documents information about the system's limitations and options for human oversight related to this AI system. The documentation is good enough to assist those who need to make decisions based on the system's outputs.	GOV 1.4 MAP 2.2	Providers Article 13	
5.2 Risk Controls We document the system risk controls, including in third-party components	GOV 1.4 MAP 2.2	Providers Article 17.1	
5.3 Model Explanation The org explains the model to ensure responsible use.	GOV 1.4 MEA 2.9	Providers Article 13	
5.4 Repository The org inventories information about this AI system in a repository of their AI systems.	GOV 1.6		
5.5 User Transparency The org marks content as AI-generated, including when users interact with their AI and in deep fakes.			Article 50
5.6 Data Transparency The org publishes a publicly available summary of the GPAI model's training data using the EU AI Office template (not yet created).			GPAI Article 53.d

Full Questionnaire:

Questions for building phases and on

6. Management Plan

The org plans how to respond to risks, including setting priorities and documenting residual risks.

	NIST	EU AI Act High risk	EU AI Act GenAI
6.1 Plan The org plans how they will respond to the risks caused by this AI system. The response options include defining the organization's risk tolerance level and deciding when risks should be mitigated, avoided, or accepted.	GOV 1.3 GOV 1.4 MAP 1.5 MAN 1.3 MAN 2.1	Provider Articles 9 17	If GPAI with systemic risk: Article 55.1b
6.2 Prioritization The org prioritizes the responses to the risks of this AI system based on impact, likelihood, available resources or methods, and the organization's risk tolerance.	GOV 1.3 MAN 1.2		
6.3 Residual Risks The org identifies the residual risks of this AI system (the risks that we do not mitigate), including risks to buyers and users of the system.	MAN 1.4		
6.4 Unexpected Risks The org has a plan for addressing unexpected risks related to this AI system as they come up.	GOV 1.4 MAN 2.1 MAN 2.3	Provider Articles 9 17	
6.5 Vulnerable Groups The org's risk management plan gives special consideration to potential adverse impacts to persons under 18y and other vulnerable groups.		Provider Article 9.9	

Full Questionnaire:
Questions for building phases and on

7. Risk Mitigation
The org acts to minimize risks, including addressing their prioritized risks and tracking incidents.

	NIST	EU AI Act High risk	EU AI Act GenAI
7.1 Meets Objectives The org proactively evaluates whether this system meets its stated objectives and whether its development or deployment should proceed.	MAN 1.1 GOV 1.5	Provider Articles 9 17	If GPAI with systemic risk: Article 55.1b
7.2 Bias & Fairness The org ensures this AI's bias and fairness performance stays meets their standards.	MAN 1.3 MAN 4.2 MEA 2.11	Provider Articles 9 10 17	
7.3 Privacy The org ensures this AI's privacy performance meets their standards.	MAN 1.3 MEA 2.10 MAN 4.2	Provider Articles 9 10 17	
7.4 Environment The org ensures this AI's environmental performance meets their standards.	MAN 1.3 MEA 2.12 MAN 4.2	Provider Articles 9 17	
7.5 Transparency & Accountability The org ensures this AI's transparency and accountability meets their standards.	MAN 1.3 MEA 2.8 MAN 4.2	Provider Articles 9 17	
7.6 Security The org ensures this AI's security and resilience meets their standards.	MAN 1.3 MEA 2.7 MAN 4.2	Provider Articles 9 17	

Full Questionnaire:

Questions for building phases and on

7. Risk Mitigation (continued)

The org acts to minimize risks, including addressing your prioritized risks and tracking incidents.

	NIST	EU AI Act High risk	EU AI Act GenAI
7.7 Explainability The org ensures this AI's explainability performance meets their standards.	MAN 1.3 MEA 2.9 MAN 4.2	Provider Articles 9	
7.8 Third Party The org ensures this AI's third-party impacts, such as IP infringement, meet their standards.	MAN 3.1 GOV 6.1 MAN 1.3	Provider Articles 9 17	
7.9 Human Oversight The org implements processes for human oversight related to this AI system.	GOV 3.2 MAP 3.5 MAN 1.3	Provider & Deployer Articles 9 14 17 26.2	
7.10 Appeal The org implements processes for appeal related to this AI system.	MAN 4.1		
7.11 End of Life The org maintains end-of-life mechanisms to supersede, disengage, or deactivate this AI system if its performance or outcomes are inconsistent with the intended use.	GOV 1.7	Provider Articles 9 17	
7.12 Safety The org ensures this AI system is safe.	MAN 1.3 MEA 2.6 MAN 4.2	Provider Articles 9 17	

Full Questionnaire:

Questions for building phases and on

7. Risk Mitigation (continued)

The org acts to minimize risks, including addressing your prioritized risks and tracking incidents.

	NIST	EU AI Act High risk	EU AI Act GenAI
7.13 Other Risks The org addresses all other risks prioritized in their plans related to this system by conducting measurable activities.	MAN 1.3 MAN 4.2	Provider Articles 9 17	
7.14 Unexpected Risks The org addresses unexpected risks related to this system by conducting measurable activities.	MAN 2.3	Provider 9 17	
7.15 Errors & Incidents The org tracks and respond to errors and incidents related to this system by conducting measurable activities.	MAN 4.3 GOV 4.3	Provider 17.1i 73	If GPAI with systemic risk: Article 55.1c
7.16 Input Diversity Consultations with diverse domain experts and end users inform risk management activities.	MEA 1.3 MEA 3.3 MEA 4.1 MEA 4.2 MEA 4.3 GOV 5.2 GOV 3.1		

Full Questionnaire:
Questions for deployment phases

8. Pre-deployment checks
The org only releases features that meet their AI ethics standards.

	NIST	EU AI Act High risk	EU AI Act GenAI
8.1 Valid and Reliable The org ensures that this system and its features are valid, reliable, and meet our standards.	MAN 1.1 MEA 2.5	Provider & Deployer Articles 15 26	
8.2 Documentation The org has all the documentation required by law.	MAN 1.1 MEA 2.5	Provider & Deployer Articles 11 12 13 16 17 18.1 26.6 48 49 71	If GPAI: Article 53 If GPAI with systemic risk: Article 55, Annex IX
8.3 Compliance The org ensures that their system is compliant with all relevant laws and standards.		Providers & Developer Articles 20 26 43 72	If GPAI: Article 53.c
8.4 Certification The systems has all relevant certificates.		Provider Article 47, Annex V	

Full Questionnaire:

Questions for deployment phases

8. Pre-deployment checks

The org only releases features that meet their AI ethics standards.

	NIST	EU AI Act High risk	EU AI Act GenAI
8.5 Communication The org has procedures for communication with all relevant stakeholders.	MAN 1.1 MEA 2.5	Provider & Deployer Articles 9 13 17 25 26 73	If Human AI Interaction Article 50

Full Questionnaire:
Questions for deployment phases

9. Monitoring The org monitors and resolve issues as they arise.			
9.1 Monitoring Plan The org plans how to monitor risks related to this system post-deployment.	MAN 4.1 GOV 1.3	Provider Article 72	
9.2 Functionality The org implements our monitoring plan, including monitoring this system's functionality and behavior post-deployment.	MEA 2.4 MEA 2.6	Provider & Deployer Articles 26.5 72	
9.3 Sustain Value The org applies mechanisms to sustain the value of this system post-deployment.	MAN 2.2		
9.4 User Input The org captures and evaluates input from users about this system post-deployment.	MAN 4.1 GOV 5.2	Provider Article 72	
9.5 Appeal and Override The org monitors appeal and override processes related to this system post-deployment.	MAN 4.1 MEA 2.6		

Full Questionnaire:
Questions for deployment phases

9. Monitoring (continued)
The org monitors and resolves issues as they arise.

	NIST	EU AI Act High risk	EU AI Act GenAI
9.6 Incidents The org monitors incidents related to this system and responds to them post-deployment	MAN 4.1 GOV 4.3 MEA 2.6	Provider & Deployer Articles 26.5 73 79	If Human AI Interaction Article 50
9.7 Third Party The org monitors incidents related to third-party components, such as pre-trained models or data, and responds to them, especially when these components are high risk.	GOV 6.2 MEA 2.6 MAN 3.1 MAN 3.2		
9.8 Other The org implements all other components of our post-deployment monitoring plan for the system.	MAN 4.1 MEA 2.6		
9.9 End of Life The org monitors issues that would trigger our end of life mechanisms for this system, and we take the system offline if issues come up.	MAN 2.4 MAN 4.1 MEA 2.6	Provider Article 73	

4

Additional Resources

Additional support **Workshop**

Workshop for additional support

We are offering a two-week workshop in which participants will learn how to evaluate AI governance using the framework and apply it to AI products their company is developing or procuring.

Participants will finish this workshop with:

- A document describing the responsibility level of their AI product to be used internally, with clients, or for external visibility.
- Actionable steps for improvement.
- Ways to leverage AI responsibility activities to improve their ability to develop, buy, and sell AI tools.
- A certificate of completion from TechBetter

The workshop is for anyone involved with developing or procuring AI:

Executives, product managers, compliance officers, HR Managers, software developers, and anyone else involved in developing of procuring AI-enabled products.

Registration and additional information

Visit https://www.techbetter.ai/workshops

Further Reading

About the TechBetter framework

All materials related to this framework are available at
www.techbetter.ai/rai-maturity-model

The materials include the following:

- **IEEE report** - Highlights of the NIST-based version of the framework
- **Academic paper** - The rationale and scholarship behind the framework
- **All Tech is Human hackathon report** - Case studies of using the framework to evaluate companies' AI governance externally, based on publicly available information
- **AI4Gov hackathon report** - Case studies of using the framework to evaluate AI governance internally in early-stage projects
- **Light-It case study** - Reflections from a company that used the framework to self-evaluate

About The EU AI Act

- The full text of the EU AI Act is available on the website of the European Parliament

- The Future of Life Institute (FLI) put together a website dedicated to the EU AI Act. It contains many helpful resources, including the following: The AI Act Explorer, which offers a convenient way to browse through the Act, Compliance checker, and The EU AI Act newsletter

- The International Association of Privacy Professionals (IAPP) creates guides about the EU AI Act. You can find them in a dedicated page in the IAPP resource library. It includes: Timeline for implementation, Compliance matrix, and Stakeholder map

About The NIST AI RMF

- The full RMF is here
- Here you can find NIST's related resources, which include the academic paper on which this framework is based

For More
And to get in touch

Ravit Dotan, TechBetter

www.techbetter.ai

/ravit-dotan

/company/techbetter

More Resources

To learn more about the framework, including more case studies, visit: https://www.techbetter.ai/rai-maturity-model

For more AI ethics resources, visit: https://www.techbetter.ai/resources

Get in Touch

For support in implementing this process in your organization, hosting workshops at your event, or speaking engagements, contact us at contact@techbetter.ai