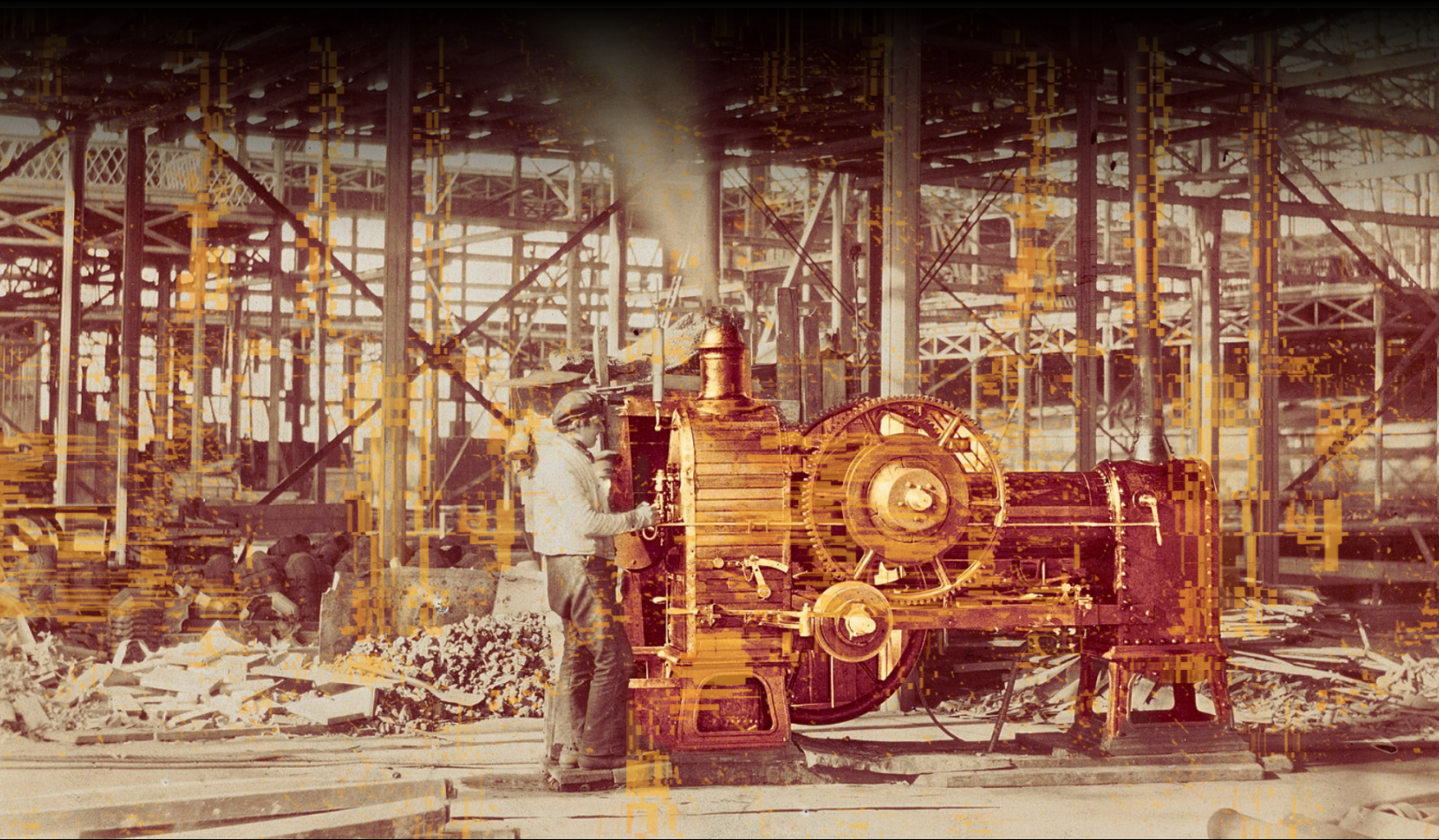


U C B E R K E L E Y

C E N T E R F O R L O N G - T E R M C Y B E R S E C U R I T Y



Mapping Key Standards and Regulations to the General-Purpose AI Risk Management Standards Profile V1.2

NADA MADKOUR | JESSICA NEWMAN | DEEPIKA RAMAN | KRISTAL JACKSON
EVAN R. MURPHY | CHARLOTTE YUAN

Cover art: The cover image is an adaptation of a photograph titled, “Steam Engine near the Grand Transept, Crystal Palace,” taken by the photographer Philip Henry Delamotte in 1851. The impact of artificial intelligence and especially general purpose artificial intelligence is often compared to the impact of the steam engine during the Industrial Revolution, which brought enormous economic gains, but also dangerous workplaces and horrible living conditions for many. The Crystal Palace housed the Great Exhibition of 1851, where examples of technology developed in the Industrial Revolution were put on display for thousands of people to see. While enjoyed by many, the Crystal Palace was also critiqued for representing a false utopia. Similarly, the rise of general purpose AI is often discussed with utopian visions, but such positive visions are often overpromised and will not be possible without the establishment of meaningful risk management strategies. The image is a reminder of the entanglement of people and machines, and the profound and lasting impact of general purpose technologies on society.

In this adaptation, the updated golden palette alludes to contemporary narratives of an “AI gold rush,” reflecting the rapid investment, aspiration, and momentum surrounding AI development. The radiant gold machinery draws the viewer’s eye and underscores how technological systems increasingly occupy the locus of attention within public and policy discourse, often overshadowing the human figure within the frame. Against this backdrop of acceleration and possibility, we present the second annual update to the AI Risk-Management Standards Profile for General-Purpose AI Systems (GPAIS) and Foundation Models (Version 1.2).

Mapping Key Standards and Regulations to the General-Purpose AI Risk Management Standards Profile V1.2

NADA MADKOUR[†] • JESSICA NEWMAN[†] • DEEPIKA RAMAN[†] • KRYSTAL JACKSON[†]
EVAN R. MURPHY[†] • CHARLOTTE YUAN[†]

[†] AI Security Initiative, Center for Long-Term Cybersecurity, UC Berkeley

All affiliations listed are either current, or were during main contributions to this work or a previous version.

Version 1.2, April 2026

For the full General Purpose AI Risk-Management Standards Profile, Version 1.2, see:

<https://cltc.berkeley.edu/publication/ai-risk-management-standards-profile-v1.2/>



Contents

INTRODUCTION	3
CHANGES FROM V1.1	3
MAPPING TO ISO/IEC 23894	4
MAPPING TO ISO/IEC 42001	6
MAPPING TO HIROSHIMA PROCESS INTERNATIONAL CODE OF CONDUCT FOR ORGANIZATIONS DEVELOPING ADVANCED AI SYSTEMS	7
MAPPING TO EU AI ACT	9
MAPPING TO EU GENERAL-PURPOSE AI CODE OF PRACTICE	12
MAPPING TO FRONTIER AI SAFETY COMMITMENTS	15
REFERENCES	17

Introduction

This document provides mappings, or “crosswalks,” between the General-Purpose Artificial Intelligence (GPAI) Risk-Management Standards Profile (GPAI Profile) and ISO AI standards (ISO/IEC 23894 and 42001), the EU AI Act, the EU General Purpose AI Code of Practice, the frontier AI safety commitments, and the Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI systems. This resource indicates how guidance in the GPAI Profile relates to clauses in these standards and regulations, making it easier to understand how these efforts relate to each other and to risk-management processes for general-purpose AI broadly. Using the guidance and resources in this document can help users of the GPAI Profile unify and standardize their AI risk management approaches. The clauses in each of the featured standards and regulations are mapped to GPAI Profile functions, categories, or subcategories that provide useful implementation guidance. However, adherence to the GPAI Profile functions, categories, or subcategories does not ensure compliance to the requirements in the mapped clauses.

Changes from V1.1

This document has been updated to reflect recent developments in the AI regulatory and governance landscape. We have made a number of changes to our policy mapping sections, including removing mappings to the White House AI Commitments and Executive Order 14110 Section 4.2, and adding mapping to the EU General-Purpose AI Code of Practice. All previously included mappings can be found in the V1.1 Mapping of the Guidance to Key Standards and Regulations (Barrett et al., 2025).

Mapping to ISO/IEC 23894

In this section, we map GPAI Profile guidance to key clauses in ISO/IEC 23894:2023, “Information technology — Artificial intelligence — Guidance on risk management.” This is based in part on the NIST draft crosswalk between the AI RMF 1.0 and ISO/IEC 23894 draft international standard (NIST, 2023). ISO/IEC 23894 provides guidance on how organizations that develop, produce, deploy, or use AI technologies can manage risk specifically related to AI, and how they can integrate risk management into their AI-related activities and functions ([ISO 2023](#)).

Table 1: Mapping between ISO/IEC 23894 and the GPAI Profile

ISO/IEC 23894 Clause	GPAI Profile Functions, Categories, or Subcategories
5.2 Leadership and commitment	Govern 1, 4
5.3 Integration	Govern
5.4 Design	Govern
5.4.1 Understanding the organization and its context	Map 1 Govern Measure
5.4.2 Articulating risk management commitment	Govern
5.4.3 Assigning organizational roles, authorities, responsibilities, and accountabilities	Govern 2
5.4.4 Allocating resources	Govern 1, 2
5.4.5 Establishing communication and consultation	Govern
5.5 Implementation	Manage
5.6 Evaluation	Measure 2.13, 3, 4
5.7 Improvement	Govern Measure Manage
6.2 Communication and consultation	Govern 2, 4, 5 Map 5.2
6.3.2 Defining the scope	Map 1
6.3.3 External and internal context	Map 1
6.3.4 Defining risk criteria	Map 1.5, 5 Measure Manage 1.1
6.4.2 Risk identification	Map 1.1, 5
6.4.2.3 Identification of risk sources	Map
6.4.2.4 Identification of potential events and outcomes	Map 5.1

MAPPING KEY STANDARDS AND REGULATIONS TO THE
GENERAL-PURPOSE AI RISK-MANAGEMENT STANDARDS PROFILE V1.2

ISO/IEC 23894 Clause	GPAI Profile Functions, Categories, or Subcategories
6.4.2.5 Identification of controls	Map Measure Manage
6.4.2.6 Identification of consequences	Map 5.1
6.4.3 Risk analysis	Map Measure
6.4.3.2 Assessment of consequences	Map 5.1 Measure
6.4.3.3 Assessment of likelihood	Map 5.1 Measure
6.4.4 Risk evaluation	Map Measure Manage
6.5 Risk treatment	Manage
6.5.2 Selection of risk treatment options	Map 1.5 Manage 1
6.5.3 Preparing and implementing risk treatment plans	Manage 2
6.6 Monitoring and review	Measure Manage 4
6.7 Recording and reporting	Govern 4 Map Measure Manage 4

Mapping to ISO/IEC 42001

In this section, we map GPAI Profile guidance to key clauses in ISO/IEC 42001:2023, “Information technology — Artificial intelligence — Management system.” This is based in part on the NIST AI RMF to ISO/IEC FDIS 42001 AI Management System Crosswalk, which was provided to NIST by Microsoft (Microsoft 2023). ISO/IEC 42001 is an international standard that specifies requirements for establishing, implementing, maintaining, and continually improving an Artificial Intelligence Management System (AIMS) within organizations (ISO 2023).

Table 2: Mapping between ISO/IEC 42001:2023 and the GPAI Profile

ISO/IEC 42001 Clause	GPAI Profile Functions, Categories, or Subcategories
4.1 Understanding the organization and its context	Govern 1 Map 1
4.3 Determining the scope of the AI management system	Map 3 Map 4 Map 5 Measure 1
4.4 AI management system	Manage
5.1 Leadership and commitment	Govern 1 Govern 2 Govern 4
5.2 AI policy	Govern 1
5.3 Roles, responsibilities, and authorities	Govern 2
6.1.2 AI risk assessment	Map 2 Map 3 Map 4 Map 5
6.1.3 AI risk treatment	Measure 1 Measure 2 Manage 1, 2
6.1.4 AI system impact assessment	Map 5
7.2 Competence	Govern 2.2
9.1 Monitoring, measurement, analysis, and evaluation	Measure Manage
10.1 Continual improvement	Manage 2 Manage 4
10.2 Nonconformity and corrective action	Govern 1.7 Manage 2.3

Mapping to the Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems

In this section, we map GPAI Profile guidance to the International Code of Conduct for Organizations Developing Advanced AI Systems, which was developed by the G7 Digital and Tech Ministers (G7 2023). This guidance aims to promote safe, secure, and trustworthy AI worldwide and provides voluntary guidance for organizations developing the most advanced AI systems, including GPAI models and generative AI systems, and builds upon the existing OECD AI Principles (G7 2023).

Table 3: Mapping between the International Code of Conduct for Organizations Developing Advanced AI Systems and the GPAI Profile

International Code of Conduct for Organizations Developing Advanced AI Systems Actions	GPAI Profile Functions, Categories, or Subcategories
1) Take appropriate measures throughout the development of advanced AI systems, including prior to and throughout their deployment and placement on the market, to identify, evaluate, and mitigate risks across the AI lifecycle.	Govern
2) Identify and mitigate vulnerabilities, and, where appropriate, incidents and patterns of misuse, after deployment, including placement on the market.	Govern 6.2 Map 2.3, 4.2, 5.1 Measure 1.1, 2.7 Manage 2.3, 4
3) Publicly report advanced AI systems' capabilities, limitations, and domains of appropriate and inappropriate use, to support ensuring sufficient transparency, thereby contributing to increased accountability.	Govern 4.2, 4.3 Map 1.1, 1.5, 2, 3, 4.1, 5.1 Measure 2, 3.1, 4.2 Manage 2.3, 2.4
4) Work towards responsible information sharing and reporting of incidents among organizations developing advanced AI systems, including with industry, governments, civil society, and academia.	Govern 2.1, 4.2, 4.3, 5 Map 1.1, 1.6, 2, 3.1, 3.2, 4.2 Measure 1, 2.8, 2.9, 3.1, 4 Manage 2.4

MAPPING KEY STANDARDS AND REGULATIONS TO THE
GENERAL-PURPOSE AI RISK-MANAGEMENT STANDARDS PROFILE V1.2

International Code of Conduct for Organizations Developing Advanced AI Systems Actions	GPAI Profile Functions, Categories, or Subcategories
5) Develop, implement and disclose AI governance and risk management policies, grounded in a risk-based approach – including privacy policies, and mitigation measures.	Govern Map 1 Measure 1 Manage 1, 2, 4
6) Invest in and implement robust security controls, including physical security, cybersecurity and insider threat safeguards across the AI lifecycle.	Govern 1.5, 1.7, 2.1, 6.2 Map 4.2, 5.1 Measure 1.1, 2.7, 2.10 Manage 1.3, 4
7) Develop and deploy reliable content authentication and provenance mechanisms, where technically feasible, such as watermarking or other techniques to enable users to identify AI-generated content.	Govern 1.6, 4.2 Map 2.1 Measure 2.7, 2.9
8) Prioritize research to mitigate societal, safety and security risks and prioritize investment in effective mitigation measures.	Govern 3.1
9) Prioritize the development of advanced AI systems to address the world’s greatest challenges, notably but not limited to the climate crisis, global health and education.	Govern 1.2, 5.2 Map 3.1, 5

Mapping to the EU AI Act

In this section, we map GPAI Profile guidance to relevant provisions represented by the EU AI Act articles (EP 2024). The EU AI Act includes regulatory requirements for GPAI models, GPAI models with systemic risk, and high-risk AI systems. At a minimum, GPAI models (or at least one or more subsets of GPAI models identified to have high-impact capabilities) are subject to requirements for transparency, and for assessing, mitigating, and documenting several types of reasonably foreseeable risks. The EU AI Act classifies high-risk AI systems as those that are either used as security components, are themselves products covered by EU legislation in Annex I of the EU AI Act, or are systems listed in Annex III (e.g., systems used for biometrics, education, law enforcement, and others). GPAI models with systemic risk (GPAISR) are classified as models with high impact capabilities. The GPAI Profile functions, categories, or subcategories mapped to EU AI Act provisions addressing high-risk AI systems or GPAISR contain relevant implementation guidance that supports the requirements set forth in these provisions. However, adherence to the mapped functions, categories, or subcategories does not guarantee compliance to the mapped EU AI Act Articles.

Table 4: Mapping between the EU AI Act and the GPAI Profile

EU AI Act Provisions (with relevance to GPAI models)	GPAI Profile Functions, Categories, or Subcategories
Chapter III: High-Risk AI System	
Section 1: Classification of AI Systems as High-Risk	
Article 6: Classification Rules for High-Risk AI Systems	Map 1.1, 2, 3, 4, 5.1
Section 2: Requirements for High-Risk AI Systems	
Article 8: Compliance with Requirements	Govern 1.1, 1.3, 1.4 Map 1.1, 1.3 Measure 2.1 Manage 2.3
Article 9: Risk Management System	Map Measure Manage
Article 10: Data and Governance	Map 1.1,2.1, 2.3, 4.1 Measure 2.2, 2.6, 2.8, 2.10, 2.11
Article 11: Technical Documentation	Map 1.1, 1.5, 2, 3, 4 Measure 1, 2, 3, 4 Manage 3.1, 4

MAPPING KEY STANDARDS AND REGULATIONS TO THE
GENERAL-PURPOSE AI RISK-MANAGEMENT STANDARDS PROFILE V1.2

EU AI Act Provisions (with relevance to GPAI models)	GPAI Profile Functions, Categories, or Subcategories
Article 13: Transparency and Provision of Information Deployers	Govern 4.2 Map 1.1, 1.6, 2, 3 Measure 2, 4 Manage 1.3, 1.4, 4.3
Article 14: Human Oversight	Govern 2.1, 2.2, 3, 5 Map 1.2, 2.2, 3.5, 5.2 Measure 1.3, 2, 3.3, 4.2 Manage 2.4, 4.1, 4.3
Article 15: Accuracy Robustness and Cybersecurity	Govern 1.2, 4.1 Map 2.3 Measure 1.1, 2, 4.2 Manage 4.1
Section 3: Obligations of Providers and Deployers of High-Risk AI Systems and Other Parties	
Article 16: Obligations of Providers of High-Risk AI Systems	Govern 1 Map 2 Measure Manage 1, 2.2, 2.4, 4
Article 17: Quality Management System	Govern 1, 2, 3.1, 4.2, 4.3, 5.1 Map 1.1, 4.1, 4.2 Measure 1, 2, 3.1, 4 Manage 1.1, 1.3, 2.1, 2.4, 3.2, 4.1
Article 20: Corrective Actions and Duty of Information	Manage 2.4
Article 25: Responsibilities along the AI Value Chain	Govern 2.1
Article 26: Obligations of Deployers of High-Risk AI Systems	Govern 1, 2.1, 2.2, 4.2, 4.3 Map 2.2, 2.3, 3.4, 3.5 Measure 2.7, 2.10, 2.13 Manage 2.4, 4.3
Article 27: Fundamental Rights Impact Assessment for High-Risk AI Systems	Govern 3.2 Map 1.1, 1.2, 1.6, 2.2, 3.5, 4, 5 Measure 2, 3, 4.1, 4.3 Manage 1, 2.4, 4.1
Section 5: Standards, Conformity Assessment, Certificates, Registration	
Article 43: Conformity Assessment	Govern 1.1, 4.1
Chapter IV: Transparency Obligations for Providers and Deployers of Certain AI Systems and GPAI Models	
Article 50: Transparency Obligations for Providers and Users of Certain AI Systems and GPAI Models	Govern 1.2 Map 2.1, 2.3 Measure 2.8, 2.7 Manage 1.3, 4.3

MAPPING KEY STANDARDS AND REGULATIONS TO THE
GENERAL-PURPOSE AI RISK-MANAGEMENT STANDARDS PROFILE V1.2

EU AI Act Provisions (with relevance to GPAI models)	GPAI Profile Functions, Categories, or Subcategories
Chapter V: General Purpose AI Models	
Section 1: Classification Rules	
Article 51: Classification of General-Purpose AI Models as General Purpose AI Models with Systemic Risk	Map 1.1, 2, 3.3 Measure 2.1, 2.9
Section 2: Obligations for Providers of General Purpose AI Models	
Article 53: Obligations for Providers of General Purpose AI Models	Govern 1.2, 4.2, 4.3 Map 1.1, 3.5, 5.1 Measure 1.1, 2.11 Manage 1, 2.2, 2.4, 4
Section 3: Obligations for Providers of General Purpose AI Models with Systemic Risk	
Article 55: Obligations for Providers of General-Purpose AI Models with Systemic Risk	Govern 4.2, 4.3 Map 1.1, 5.1 Measure Manage 1, 2, 4
Chapter IX: Post-Market Monitoring, Information Sharing, Market Surveillance	
Section 1: Post-Market Monitoring	
Article 72: Post-Market Monitoring by Providers and Post-Market Monitoring Plan for High-Risk AI Systems	Manage 2, 3, 4
Article 73: Reporting of Serious Incidents	Manage 2.3, 4.1, 4.3
Article 78: Confidentiality	Govern 6.1 Map 4.1 Measure 2.10

Mapping to the EU General-Purpose AI Code of Practice

In this section, we map GPAI Profile to the EU General-Purpose AI (GPAI) Code of Practice (EC 2025) Transparency, Copyright, and Safety and Security Chapters.¹ The Code of Practice helps industry comply with the EU AI Act legal obligations on safety, transparency, and copyright of general-purpose AI models (EC 2025).

Table 5: Mapping between the EU General Purpose AI (GPAI) Code of Practice and the GPAI Profile

General Purpose AI (GPAI) Code of Practice Measures	GPAI Profile Functions, Categories, or Subcategories
Transparency Chapter	
Commitment 1: Documentation	
Measure 1.1 Drawing up and keeping up-to-date model documentation	Govern 4.2 Map 1.1 Measure 2.9, 3.1 Manage 4.1
Measure 1.2 Providing relevant information	Govern 4.2, 4.3 Map 1.5, 2.2 Manage 1.4
Copyright Chapter	
Commitment 1: Copyright policy	
Measure 1.1 Draw up, keep up-to-date and implement a copyright policy	Govern 1.1
Measure 1.2 Reproduce and extract only lawfully accessible copyright-protected content when crawling the World Wide Web	Govern 1.1 Measure 2.10
Measure 1.3 Identify and comply with rights reservations when crawling the World Wide Web	Govern 1.1 Measure 2.10
Measure 1.4 Mitigate the risk of copyright-infringing outputs	Govern 6.1 Map 4.1
Measure 1.5 Designate a point of contact and enable the lodging of complaints	Govern 2.1, 5.1

¹ Reporting frequency and channels, notification timelines, and other measures that are solely meant to demonstrate compliance with the expectations of the EU AI Office are not mapped in this table since the GPAI Profile aims to provide overarching guidance that can be adopted across contexts.

MAPPING KEY STANDARDS AND REGULATIONS TO THE
GENERAL-PURPOSE AI RISK-MANAGEMENT STANDARDS PROFILE V1.2

General Purpose AI (GPAI) Code of Practice Measures	GPAI Profile Functions, Categories, or Subcategories
Safety and Security Chapter	
Commitment 1: Safety and Security Framework	
Measure 1.1 Creating the Framework	Govern 1, 2.1, 5, 6
Measure 1.2 Implementing the Framework	Map 1.1, 4.1, 5.1 Measure 1.1, 1.2, 2, 3.1, 3.2, 4 Manage 1.1, 1.2, 1.3, 4.1, 4.3
Measure 1.3 Updating the Framework	Govern 1.5 Measure 1.2, 3.1
Commitment 2: Systemic risk identification	
Measure 2.1 Systemic risk identification process	Govern 4.2 Map 1.1, 5.1 Manage 4.1
Measure 2.2 Systemic risk scenarios	Map 5.1
Commitment 3: Systemic risk analysis	
Measure 3.1 Model-independent information	Map 1.1
Measure 3.2 Model evaluations	Measure 1.1, 1.3, 2.2
Measure 3.3 Systemic risk modelling	Map 5.1
Measure 3.4 Systemic risk estimation	Map 5.1
Measure 3.5 Post-market monitoring	Measure 3.2 Manage 4.1, 4.3
Commitment 4: Systemic risk acceptance determination	
Measure 4.1 Systemic risk acceptance criteria and acceptance determination	Map 1.5 Measure 2.6
Measure 4.2 Proceeding or not proceeding based on systemic risk acceptance determination	Manage 1.1
Commitment 5: Safety mitigations	
Measure 5.1 Appropriate safety mitigations	Map 3.5 Manage 1.2, 1.3
Commitment 6: Security mitigations	
Measure 6.1 Security goal	Map 4.2
Measure 6.2 Appropriate security mitigations	Map 4.2 Measure 2.7 Manage 1.2, 1.3
Commitment 7: Safety and security model reports	
Measure 7.1 Model description and behaviour	Map 1.1, 1.3, 2.1, 2.2, 3
Measure 7.2 Reasons for proceeding	Manage 1.1

MAPPING KEY STANDARDS AND REGULATIONS TO THE
GENERAL-PURPOSE AI RISK-MANAGEMENT STANDARDS PROFILE V1.2

General Purpose AI (GPAI) Code of Practice Measures	GPAI Profile Functions, Categories, or Subcategories
Measure 7.3 Documentation of systemic risk identification, analysis, and mitigation	Govern 1.4, 4.2 Map 1.1, 2.3, 5 Measure 1, 2 Manage 1.2, 1.3, 1.4
Measure 7.4 External reports	Govern 5.1, Measure 1.1, 1.3
Measure 7.5 Material changes to the systemic risk landscape	Manage 1.3, 1.4
Measure 7.6 Model report updates	Manage 4.1
Commitment 8: Systemic risk responsibility allocation	
Measure 8.1 Definition of clear responsibilities	Govern 1.5, 2.1, 3.2
Measure 8.2 Allocation of appropriate resources	Govern 1.3 Manage 2.1
Measure 8.3 Promotion of a healthy risk culture	Govern 4.1 Map 5.2
Commitment 9: Serious incident reporting	
Measure 9.1 Methods for serious incident identification	Govern 4.2, 4.3, 6.2 Map 5.1
Measure 9.2 Relevant information for serious incident tracking, documentation, and reporting	Govern 4.3, 6.2
Commitment 10: Additional documentation and transparency	
Measure 10.1 Additional documentation	Govern 1.4, 2.1 Map 2. 4, 5.1, 5.2 Measure 1, 2
Measure 10.2 Public transparency	Govern 4.2, 4.3 Map 2.2

Mapping to the Frontier AI Safety Commitments

In this section, we map GPAI Profile guidance to the Frontier AI Safety Commitments (DSIT 2024), a set of voluntary commitments that were made by notable AI companies at the AI Seoul Summit in May 2024 to support safe and trustworthy development and use of frontier AI models and systems.

Table 6: Mapping between the Frontier AI Safety Commitments and the GPAI Profile

Frontier AI Safety Commitments	GPAI Profile Functions, Categories, or Subcategories
<p>Outcome 1. Organisations effectively identify, assess, and manage risks when developing and deploying their frontier AI models and systems. They will:</p>	
<p>I. Assess the risks posed by their frontier models or systems across the AI lifecycle, including before deploying that model or system, and, as appropriate, before and during training. Risk assessments should consider model capabilities and the context in which they are developed and deployed, as well as the efficacy of implemented mitigations to reduce the risks associated with their foreseeable use and misuse. They should also consider results from internal and external evaluations as appropriate, such as by independent third-party evaluators, their home governments, and other bodies their governments deem appropriate.</p>	<p>Govern 4.2, 5 Map 1.1, 1.3, 1.4, 1.5, 1.6, 2, 3, 4, 5 Measure</p>
<p>II. Set out thresholds at which severe risks posed by a model or system, unless adequately mitigated, would be deemed intolerable. Assess whether these thresholds have been breached, including monitoring how close a model or system is to such a breach. These thresholds should be defined with input from trusted actors, including organisations’ respective home governments as appropriate. They should align with relevant international agreements to which their home governments are party. They should also be accompanied by an explanation of how thresholds were decided upon, and by specific examples of situations where the models or systems would pose intolerable risk.</p>	<p>Govern 1.1, 1.3, 1.4 Map 1.5, 1.6 Measure 1, 2</p>
<p>III. Articulate how risk mitigations will be identified and implemented to keep risks within defined thresholds, including safety- and security-related risk mitigations such as modifying system behaviours and implementing robust security controls for unreleased model weights.</p>	<p>Map 2.1 Measure 1, 2 Manage 1, 2, 3, 4</p>

MAPPING KEY STANDARDS AND REGULATIONS TO THE
GENERAL-PURPOSE AI RISK-MANAGEMENT STANDARDS PROFILE V1.2

Frontier AI Safety Commitments	GPAI Profile Functions, Categories, or Subcategories
IV. Set out explicit processes they intend to follow if their model or system poses risks that meet or exceed the pre-defined thresholds. This includes processes to further develop and deploy their systems and models only if they assess that residual risks would stay below the thresholds. In the extreme, organisations commit not to develop or deploy a model or system at all if mitigations cannot be applied to keep risks below the thresholds.	Govern 1.7 Manage 1.1, 1.3, 2.4
V. Continually invest in advancing their ability to implement commitments I-IV, including risk assessment and identification, thresholds definition, and mitigation effectiveness. This should include processes to assess and monitor the adequacy of mitigations, and identify additional mitigations as needed to ensure risks remain below the pre-defined thresholds. They will contribute to and take into account emerging best practice, international standards, and science on AI risk identification, assessment, and mitigation.	Measure 3 Manage 4
Outcome 2. Organisations are accountable for safely developing and deploying their frontier AI models and systems. They will:	
VI. Adhere to the commitments outlined in I-V, including by developing and continuously reviewing internal accountability and governance frameworks and assigning roles, responsibilities, and sufficient resources to do so.	Govern 1.5, 1.6, 2, 3.2
Outcome 3. Organisations' approaches to frontier AI safety are appropriately transparent to external actors, including governments. They will:	
VII. Provide public transparency on the implementation of the above (I-VI), except insofar as doing so would increase risk or divulge sensitive commercial information to a degree disproportionate to the societal benefit. They should still share more detailed information which cannot be shared publicly with trusted actors, including their respective home governments or appointed body, as appropriate.	Govern 1.4, 4.3
VIII. Explain how, if at all, external actors, such as governments, civil society, academics, and the public are involved in the process of assessing the risks of their AI models and systems, the adequacy of their safety framework (as described under I-VI), and their adherence to that framework.	Govern 5 Map 5 Measure 3.3, 4 Manage 4

References

- Anthony M. Barrett, Jessica Newman, Brandie Nonnecke, Nada Madkour, Dan Hendrycks, Evan R. Murphy, Krystal Jackson, and Deepika Raman (2025) Mapping Of The AI Risk-Management Standards Profile for General-Purpose AI (GPAI) and Foundation Models V1.1 Guidance To Key Standards And Regulations. UC Berkeley Center for Long-Term Cybersecurity, <https://cltc.berkeley.edu/wp-content/uploads/2025/01/Berkeley-Mapping-of-Profile-Guidance-v1-1-to-Key-Standards-and-Regulations.pdf>
- DSIT (2024) Frontier AI Safety Commitments. In AI Seoul Summit 2024. UK Department for Science, Innovation & Technology, <https://www.gov.uk/government/publications/frontier-ai-safety-commitments-ai-seoul-summit-2024/frontier-ai-safety-commitments-ai-seoul-summit-2024>
- EC (2025) The General-Purpose AI Code of Practice. European Commission, <https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai>
- EP (2024) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). European Parliament, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>
- G7 (2023) Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems. G7 2023 Hiroshima Summit, <https://www.mofa.go.jp/files/100573473.pdf>
- Nada Madkour, Jessica Newman, Deepika Raman, Krystal Jackson, Evan R. Murphy, Charlotte Yuan, Dan Hendrycks (2026) General Purpose AI Risk-Management Standards Profile, Version 1.2. UC Berkeley Center for Long-Term Cybersecurity, <https://cltc.berkeley.edu/publication/ai-risk-management-standards-profile-v1.2/>
- Microsoft (2023) NIST AI Risk Management Framework to ISO-IEC-42001 Crosswalk. Microsoft, https://airc.nist.gov/docs/NIST_AI_RMF_to_ISO_IEC_42001_Crosswalk.pdf
- NIST (2023) Crosswalk AI RMF (1.0) and ISO/IEC FDIS 23894 Information technology - Artificial intelligence - Guidance on risk management. National Institute of Standards and Technology, <https://www.nist.gov/document/ai-rmf-crosswalk-iso>
- NIST (2024) Managing Misuse Risk for Dual-Use Foundation Models, Initial Public Draft. NIST AI 800-1 ipd. National Institute of Standards and Technology, <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.800-1.ipd.pdf>



CLTC

Center for Long-Term
Cybersecurity

UC Berkeley