Three key steps for artificial intelligence (AI) governance

Shape the future with confidence

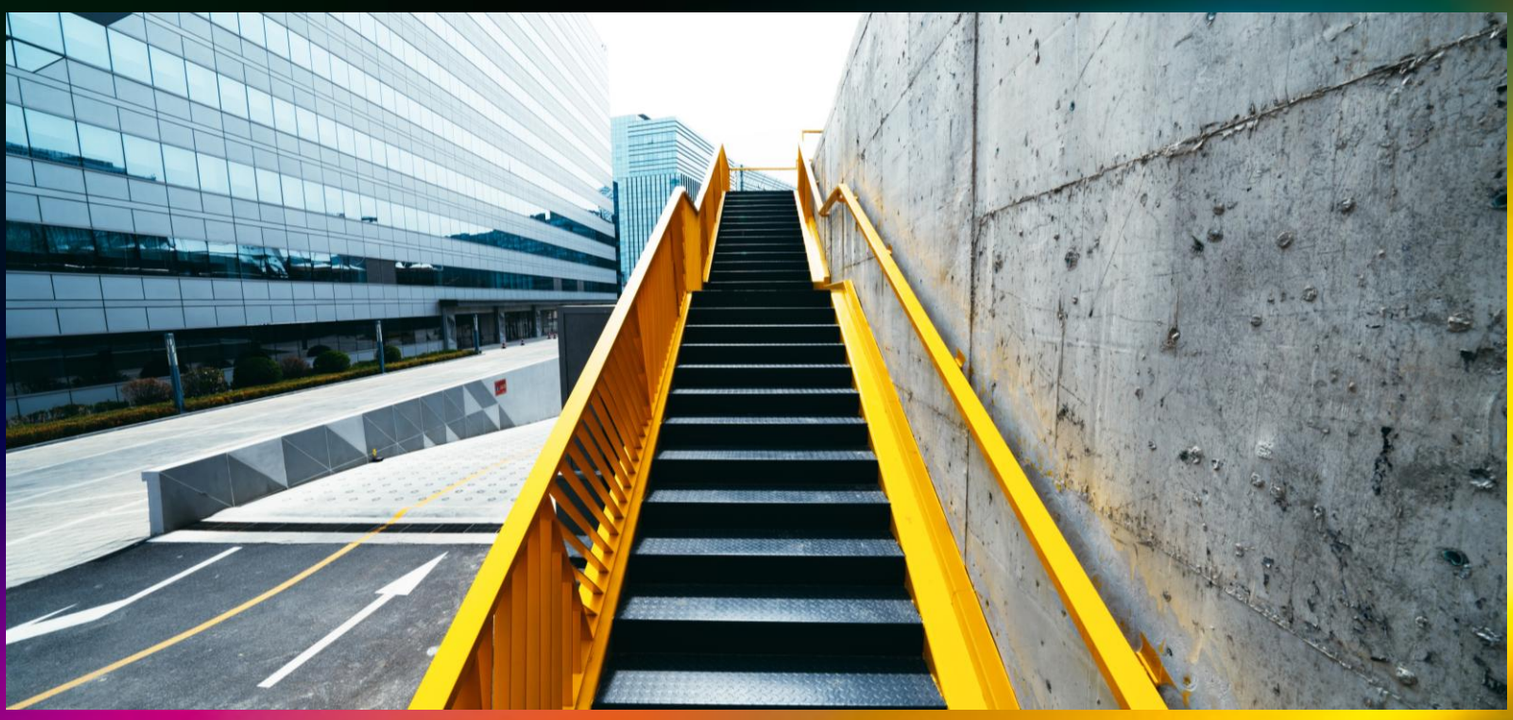
AI and its governance: prepare now

The use of artificial intelligence has become an integral part of our daily lives, changing the way we work and live and providing new opportunities for organizations to increase efficiency and innovation. Regulators expect firms to leverage existing management frameworks to identify and address the new risks that AI present. Which means that risk teams need to work quickly to understand the overlap with existing control environments and fill any gaps.

> “
> By 2026, most global firms will recognize AI risk as a principal risk.
>
> Matt Whalley

There are three steps to understanding the overlap with your existing risk management framework, and to fill out any gaps. The first step is to define what you mean by “AI risk”, and what drives it. The second step is to create a specific set of AI risk controls. Your new AI risk control framework will enable you to test the readiness of your existing policies, processes and procedures to manage the emerging risks presented by AI. The third step will involve implementing AI risk assessments to help you understand and prioritise necessary compliance activity.

This short paper sets out a working definition of AI risk, a set of seven AI risk drivers, and ten AI risk control domains as well as six broad categories of question to include in your risk assessments. To access the full AI risk control framework, and review our risk assessment tool, please get in touch via the contacts provided.



Step 1: Defining AI Risk

At a "policy-level", define AI risk in terms of the form of loss you want to prevent, and what could enable that loss to happen. Our working definition is below:

> "AI risk is the potential for adverse impacts and uncertainties arising from the failure to develop, distribute, deploy, or use AI technologies in accordance with responsible or ethical practices, or legal and regulatory obligations. This risk materializes when the use of AI results in unacceptable negative outcomes for individuals, society, the environment or the planet.

A succinct policy-level definition is a great start, but to implement the definition at an operational level you need to refine the scope further to recognize the specific activities that could drive AI risk in your organization. We created seven risk drivers - listed in the table below - by reviewing several sources of information including the EU AI Act, NIST2 Framework, OECD Principles, and Responsible AI principles. Responsible AI principles are mapped in the second column, as a cross-check to see whether there are any obvious gaps or overlaps in the drivers identified.

	Risk driver	Responsible AI principles
01	Failure to supply or adopt AI that is explainable, transparent, fair, reliable, secure, sustainable and privacy aware	Accountability; Transparency; Fairness; Sustainability; reliability; Explainability; Security; Privacy Aware
02	Failure to ensure that datasets leveraged by AI are properly managed and comply with applicable legal and ethical standards	Reliability; Fairness; Privacy Aware; Compliance; Security
03	Failure to adequately assess the potential detriment current or future use of AI could have on humans, the environment, society or the planet	Accountability; Transparency; Sustainability
04	Failure to continuously monitor and assess the impact of AI operations	Accountability; Compliance; Transparency; Explainability; Sustainability; Reliability
05	Failure to adequately inform and or obtain consent from individuals interacting with or influenced by AI	Transparency; Compliance; Security
06	Failure to adequately understand and comply with current and evolving AI laws and regulations relevant to your business operations	Compliance; Accountability; Reliability
07	Failure to effectively and timely handle requests, complaints, and incident responses	Accountability; Privacy Aware; Compliance; Security; Reliability

Step 2: Design your risk control framework

After defining the risks you need to manage, the next step is to create a template Risk Control Framework (RCF) for AI. Our template RCF contains 10 control domains and 34 sub-domains or specific operational controls. Each Domain – shown in the table below, focuses on a common set of operational policies, procedures and processes that serve to manage AI risk. Control domains are an important architectural element which help to focus conversation with risk experts embedded in relevant operational teams. For instance, to enable discussions with legal and privacy teams regarding the management of risks that personal data may be used without consent, or the protection of intellectual property generated by organizational AI.

If you would like to access our full AI risk control framework, please get in touch. We would be happy to walk you through the 34 sub-domains in more detail.

	Control domain	Description
01	AI risk control Framework	Collection of operational procedures and protocols that align to enterprise risk management structure and serve to provide oversight, management of the risks presented by use of AI.
02	IT Governance and Ops	Collection of operational procedures, protocols and training that are specific to the IT risk management structure and serve to provide oversight, management and mitigation of the risks presented by use of AI.
03	AI inventory	A record of AI-related systems and mandatory information about their purpose, nature, scope, functionality and risk level. Operate in conjunction with AI risk assessment and model card controls.
04	AI risk assessment	Policies and procedures that embed the use of standardized risk assessments of AI systems, to aid the identification and management of potential harms or other risks that may result from the deployment and use of the AI system.
05	Rights management	Policies and procedures that establish the requirements for managing individual and non-contractual rights, including but not limited to notification requirements, rights to object/challenge decisions, consent to data-use, copyright and Intellectual property (IP) ownership.
06	Data governance / risk	Established policies, procedures and protocols to manage risks relating to the underlying data used to train and run AI. Typically include personal, confidential and other data used for training and development of models.
07	AI model card framework and technical documentation	Documentation framework detailing each AI model's purpose, data sources, training methodologies, performance metrics, and potential biases in alignment with organisation's ethical standards, legal requirements, and operational needs.
08	AI conformity and resilience monitoring	Policies, procedures and protocols required conformity assessments for AI systems to verify whether an AI system is fit for purpose, operates as expected based on its design requirements, and satisfies applicable regulatory requirements.
09	Third Party Oversight	Policies and procedures relating to requirements for managing third-party risk across the AI system supply chain.
10	Incidents and Complaints	Policy requirements and operational protocols to identify, manage and report major AI incidents and complaints.

Step 3: Implement AI Risk Assessments

AI Risk Assessments are the foundation of your AI compliance environment. They will enable you to prioritize risk control augmentation, build your AI inventory, and drive post-deployment assurance activity. The pace of change in AI means that AI risk assessments need to move quickly from the theoretical and into the practical. And continue to evolve. Our risk assessment process splits questions into six categories. And aligns your risk reports to responsible AI principles and client specific risk flags. We track/assess regulatory developments continuously, and work with clients to create specific question-sets based on our default templates.

	Category	Description
01	Parties and roles	Identify all stakeholders involved in the AI system's lifecycle and define their roles and responsibilities. This clarity is crucial for effective governance and accountability.
02	System characteristics	Detail the technical and functional aspects of the AI system, including architecture, algorithms and operational parameters. Understanding these characteristics is fundamental to assessing potential risks.
03	Data requirements	Examine the data inputs and outputs of the AI system, focusing on data sources, quality and processing practices. This section is key to evaluating risks related to data privacy and security.
04	Purpose and use	Articulate the intended use cases and objectives of the AI system, providing a basis for assessing alignment with ethical principles and regulatory requirements.
05	Individual impact	Evaluate the potential effects of the AI system on individuals and communities, considering factors like fairness, transparency and the risk of harm. This section underscores the commitment to your AI principles.
06	Safety protocols	Develop tools and guidelines for ongoing compliance monitoring, including checklists and templates aligned with current AI laws and regulations. This proactive approach facilitates continuous compliance and risk management.

To learn more about our approach to AI governance, and how our bespoke tooling can accelerate your compliance journey, please get in touch.

How EY can help

EY has created Data Permissions Navigator (DPN) to help organizations address the key issues of privacy risk management and to help ensure AI governance across your business units.

EY DPN has an intuitive user interface, data-rich reports and information dashboards, an advanced reasoning engine, thematic approvals function, and a global AI risk control framework. It will help your front-line data teams to operate effectively and efficiently, supporting you as you sustainably grow your business with AI.

AI-specific features include:

- AI risk assessments for data and AI teams
- AI Risk Control Framework to embed AI Governance
- Automated AI inventory
- Privacy Impact Assessments for privacy teams
- Automation components to consume existing compliance/control data
- Dashboards and reporting for risk owners
- Global AI and privacy legal research mapped to control libraries
- Workflow and API integration

To request a demo, or for more information contact:

Stuart Allan
Digital Risk & AI Governance Lead
EY UK Risk Consulting

Stuart.allan@uk.ey.com
+441412267383

Peter Katko
Global AI Leader for Law
EY Tax GmbH Steuerberatungsgesellschaft

peter.katko@de.ey.com
+49 89 14331 25951

Peter Bolger
Global Technology Law Leader
EY Law Ireland

peter.bolger@ie.ey.com
+35312212460

John Sharp
DPN Sales Lead
Ernst & Young LLP

john.sharp@uk.ey.com
+44207 7830 426

Bernadette Weesdorp
EMEIA Financial Sector (RAI) Leader
EY Adviseurs B.V.

bernadette.wesdorp@nl.ey.com
+31884 071 039

Matt Whalley
EY DPN Global Solution Lead
Ernst & Young LLP

mwhalley1@uk.ey.com
+44 20 7951 0296

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EYG no. 009298-24Gbl
ED None

ey.com