Conventional AI risks and large language models (LLMs) risks across the lifecycle

Ś	Data/Technology risk	Data/Technology risk	Operational risk	Operational risk
itional Al risks	Data capability	Technology capability	Business continuity	Performance drift
	Cyber risk	Conduct/Compliance risk	Model risk	
Conventional	Cyber attack and adversarial attack	Bias/Fairness	Explainability	
	Data/Technology risk	Data/Technology risk	Model risk	Reputational risk
LLM Specific risks	Data host, sharing, retention and security	Data privacy and PII Data	Hallucination	Linked to all other risks
	Legal/Regulator risk	Legal/Regulator risk		
	Lawsuit and reg penalty	Copyright		
	Third-party risk	Conduct/Compliance risk		
	LLMs provided by third party	Toxic information		
Da	ata/Technology risk 📃 Operational risk	Cyber/Legal/Regulator risk Conduct/C	ompliance risk Model/Reputational risk	Third-party risk Conduct/Compliance risk



EU AI Act overview: Risk-based approach

Unacceptable risk

All Al systems are considered a clear threat to the safety, livelihoods and rights of people, such as social scoring by governments, real-time remote biometric identification systems, etc.

High risk

Include the use of AI in employment, education, law enforcement, surveillance systems, border control, essential private and public services, and critical infrastructure (e.g., transport)

• Limited risk

Al systems with specific transparency obligations (i.e., disclosure when users are interacting with chatbots)

Minimal or no risk

Allows free use of minimal-risk AI (e.g., spam filters)

EU AI Act requirements



Prohibited with exceptions of specific uses



Subject to mandatory requirements and third-party conformity assessments



Allowed with specific limited transparency obligations



Allowed

The AI Act applies a tiered compliance system with different requirements for each tier, ranging from prohibiting certain practices to none. All AI systems must be inventoried and assessed to determine their risk category and the ensuing responsibilities.