WAVESTONE

Boardroom Briefing

AI Governance and Risk Management

2026 is the year AI governance becomes a Board mandate.

Understand why taking a proactive approach to AI risk is essential for ***protecting the business*** *and* ***securing competitive advantage.***

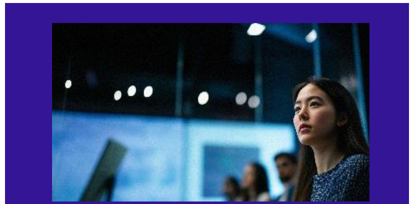
Table of Contents

Introduction

AI is advancing at a pace that outstrips traditional governance models – and **Boards must act now.**

Our experts highlight the **rapidly evolving risk landscape** and the complexity of **regulatory and compliance challenges**, then offer a **practical framework** to support the **responsible scaling of AI** across organizations.

Chapters



Client stories

About Wavestone

Executive Summary

AI risks pose an existential threat to companies; responsibility lies with all Board members.

As AI proliferates across companies and industries, **Boards must act now** to ensure their organizations are fully equipped to adopt AI but, equally importantly, to **manage the novel, and existential, risks** AI brings.

In this paper, we explain how **a lack of effective AI governance** - overseen by the Board – **poses critical threats to** the organization, whether from a regulatory, reputational or innovation perspective.

We also underline how **all Board members have responsibilities** when it comes to AI Governance, and that it is not an area for the CIO alone.

But first, a wake-up call for why this paper is an essential read for Boards:

AI is accelerating – and so is regulation. The rapid rise of AI capabilities, alongside evolving frameworks like the EU AI Act, signals the scale of the challenge. Boards must act now to steer adoption and stay in control.

Without Governance, AI innovation stalls. It's highly likely the reason the most promising AI initiatives are being paused is not technical. It's because Legal, Risk, and Compliance teams are unable to sign off in the absence of robust AI compliance and controls frameworks.

AI Governance: your license to scale. The good news is that AI Governance doesn't slow progress – it enables it.

However, this only happens when it's clearly defined and embedded into operations.

It gives Boards the visibility and structure needed to **foster collaboration and unlock innovation** across diverse teams.

Similarly, the winners will be those who **can strike the right balance** between **speed** (driving AI usage), **control** (ensuring risks are managed) and **ROI**.

In sum, **good governance is a competitive advantage**. Organizations that lead in AI will be those trusted to deploy it – by regulators, customers, and employees alike.

Mathew Wells

Associate Partner

Madeleine Thirsk

Senior Manager

> **“Boards should view AI Governance as their organization’s license to scale AI."**
>
> **Mathew Wells**

AI Governance must be on Board agendas

AI risks often 'slip through the gaps'

Lack of awareness and skills
Many organizations lack a clear understanding of their AI landscape, the risks it poses, and the standards they must meet - internally and externally, making it difficult to assess maturity or define effective governance.

Unclear mandate and ownership
Boards often face ambiguity over who is accountable for AI controls, leading to fragmented responsibility across governance and risk functions.

Insufficient capacity
AI is often treated as a peripheral task, with no dedicated roles or ownership. This leaves risks un-managed, and governance underdeveloped.

Outdated processes
Existing frameworks – like third-party risk management or IT asset reviews – rarely account for AI, creating blind spots where AI risks go unaddressed.

...but Boards that fail to get abreast of AI Governance face three critical risks

⚠ **Regulatory exposure** Without defined risk classifications, model documentation, and control processes, **compliance with laws like the EU AI Act will be impossible**.

⚠ **Reputational damage** Customers, employees, and shareholders are watching how AI is used; a misstep can **undermine trust and brand equity overnight**.

⚠ **Lost momentum** Innovation teams may build brilliant models, but without governance, these models won't be approved for deployment, **creating costly bottlenecks**.

The AI risk landscape is rapidly evolving

The world of AI presents uncertainty and opportunity, with new technologies and use-cases emerging all the time against a backdrop of risks and regulations.

Key **risk pillars**

MALICIOUS USE

Deliberate exploitation of AI for harmful purposes

Autonomous AI Agents	Deepfakes & Disinformation	Security Threats	Data Privacy & Confidentiality
Capable of performing tasks without human intervention	Can create fake content, leading to misinformation and distrust	Vulnerabilities can be exploited by malicious actors	AI data is often permissionless, causing risks

MALFUNCTIONS

Unintended failures or errors in AI

Data Quality & Reliability	Data Bias & Discrimination	Governance	Loss of Control
AI systems generating incorrect or inconsistent outputs, or 'hallucinations'	AI systems making biased decisions that harm certain groups, based on biased data	Set standards to align AI strategically, manage risks, and ensure ROI	Unpredictable AI behavior; risk amplifies with overreliance on AI

SYSTEMIC

Broader societal and economic challenges posed by AI

Regulations	Trust & Change Management	Equality
Changing AI regulations mean breaches risk fines, lost trust, and brand harm	AI misuse, bias, or failures erode trust and adoption. Models must be explainable	AI worsening or creating inequalities by favoring certain groups

Key **risk mitigations** to embed

Establish strong oversight and controls to monitor AI and verity its outputs	Advance detection tools, boost AI literacy and enforce content authenticity standards	Strengthen cybersecurity protocols to anticipate and resist adversarial attacks	Strengthen data handling to uphold privacy and confidentiality standards

Use data governance with testing, monitoring, and bias checks to manage drift and improve performance	Improve AI explainability and documentation , with checks to verify outputs and reduce bias-supporting ethical use	Extend business controls to AI and ensure robust development and testing oversight	Establish fail-safes, clear operational guidelines, and human oversight for critical AI decisions

Create adaptive regulatory frameworks with central standards and local flexibility to track global developments	Ensure AI transparency, user education and human oversight in decision-making	Adopt inclusive AI policies that ensure equal access, sustainability and energy efficiency

Addressing these challenges requires a comprehensive, ''eco-system" approach, bringing together teams from Risk, AI, Data & Analytics, Cyber and Op Resilience, Architecture, Regulatory & Compliance, Assurance, and Change Delivery.

Regulatory and compliance challenges are particularly complex

Organizations must adhere to a complex, overlapping and rapidly evolving regulatory framework - as well as emerging laws and regulations. This calls for an AI Regulatory Compliance strategy to mitigate risks and control the use of AI.

Europe

- The EU AI Act is the world's first horizontal AI regulation. It focuses on the use and risk level of AI systems, granting citizens specific rights & protections. It categorizes AI by risk.
- The UK takes a flexible, principles-based approach, relying on existing regulatory bodies to manage AI risks. It prioritizes agility and innovation, avoiding new legislation in favor of guidance & sector-specific oversight.

Middle East and Africa

- AI regulation is emerging rapidly through 'soft law' approaches and national strategies.

Americas

- AI regulation is nascent but evolving, especially in the US.
- The region leans towards a rights-based model, emphasizing transparency, accountability and mitigation of harm. Regulatory efforts are fragmented but gaining momentum.

APAC

APAC is a diverse landscape:

- China is developing vertical, state-led regulations, tailored to specific AI applications.
- Japan & Singapore favor light touch governance, promoting innovation with minimal regulatory burden.

Wavestone's Global AI Regulations Tracker enables organizations to stay compliant and protect their reputation by continuously monitoring regulatory trends and adapting through robust AI frameworks.
View: **Global AI regulations are shifting fast, but are Boards keeping up? | Wavestone**

Further complications to consider

AI definitions vary globally, with overlapping regulations often applying. Organizations must follow the strictest standards and categorize AI systems by risk - unacceptable, high, limited, or low - to guide governance.

AI regulations vary in form, scope, and enforceability - some are sector-specific, others cross-sector. With overlapping global rules, businesses must track changes and act on the strictest requirements.

Organizations must balance compliance with brand protection, meeting regulatory demands isn't enough. Non-compliance risks fines and reputational damage. Leading in AI means tracking competitors, engaging regulators, and driving progress across strategy, communications, processes and technology.

Executives have key responsibilities for AI Risk Oversight

Role-specific considerations to inform a complete and effective AI risk response

Chief Executive / Operating Officer

- Is AI strategy aligned with **business goals**?
- Is there clear **definition & visibility** of the AI estate?
- Are there **roles and checkpoints** in AI lifecycle, with accountability?
- **Regulatory and best-practice** requirements tracked and addressed?

Chief Risk Officer

- How are AI risks integrated into **risk appetite strategy** & **enterprise-risk frameworks**?
- Does the risk/ control framework cover AI risks **across the lifecycle**? Are **assessments** done?
- How does AI affect **compliance posture**? Are **regulations tracked**?

Chief Technology Officer

- What **decisions** rely on AI? Are they **explainable**?
- Who **manages and monitors** AI throughout its **lifecycle**?
- How can **reporting tools** ensure visibility and transparency?

Chief Marketing Officer

- How do **customers, investors, and employees** perceive AI? Is **feedback monitored**?
- Does the company maintain a positive AI **brand perception and reputation**?

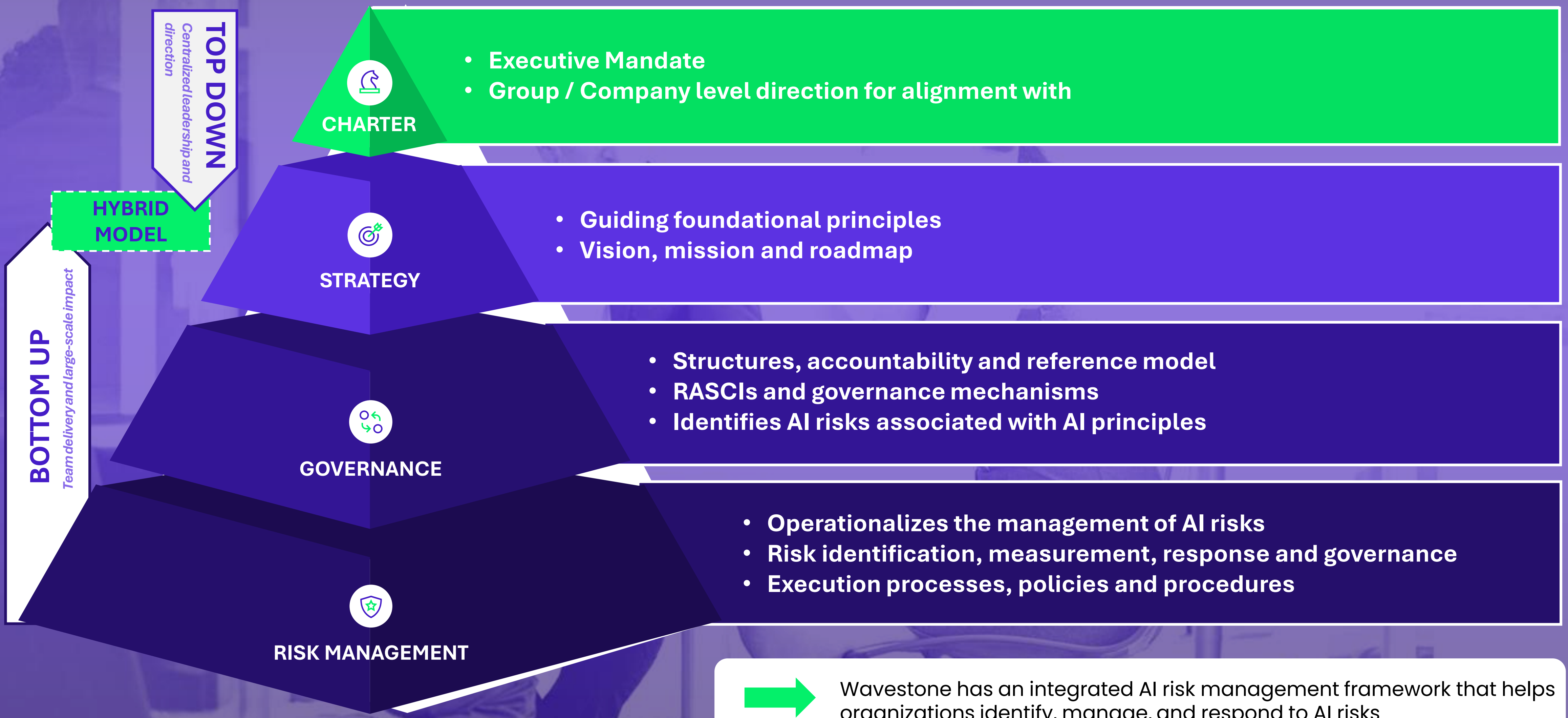
Chief Data Protection Officer

- How is AI data collected while meeting p**rivacy requirements**?
- What is the source & quality of **AI training data**? Is it free of bias?
- Are AI outputs monitored for **bias / discrimination**?

Chief Information Security Officer

- What **security safeguards** protect AI models?
- How is AI security **awareness** enforced?

The Integrated AI Risk Management Framework


TOP DOWN
Centralized leadership and direction
HYBRID MODEL
BOTTOM UP
Team delivery and large-scale impact

CHARTER

- Executive Mandate
- Group / Company level direction for alignment with

STRATEGY

- Guiding foundational principles
- Vision, mission and roadmap

GOVERNANCE

- Structures, accountability and reference model
- RASCIs and governance mechanisms
- Identifies AI risks associated with AI principles

RISK MANAGEMENT

- Operationalizes the management of AI risks
- Risk identification, measurement, response and governance
- Execution processes, policies and procedures

Wavestone has an integrated AI risk management framework that helps organizations identify, manage, and respond to AI risks

CLIENT STORY 01 Operationalizing AI governance

Client challenge

A global insurance company had recently completed the first part of its AI Governance Operationalization journey, during which core AI assets were designed.

The global lead of data quality and controls now needed to bring its AI governance framework to life across the organization, uplifting and aligning these assets with regulatory expectations and business standards to enable responsible, ethical, and compliant AI adoption at scale.

The challenge was twofold:

- Ensuring AI governance practices aligned with the company's compliance policies, global frameworks, and fast-evolving regulations (EU AI Act, NIST AI RMF).
- Embedding practical accountability and assurance mechanisms across the AI lifecycle to manage risk without slowing innovation.

Approach

A phased, collaborative approach was taken, structured around 4 key delivery stages over 12 weeks:

1. **Plan**
   - Set governance structures, roles, & comms.
   - Built Stakeholder Matrix for cross-function engagement.
   - Evidence, goals, and prioritized PoCs.
2. **Design**
   - Reviewed existing AI governance assets and requirements.
   - Completed Gap Analysis and action plan for compliance.
   - Assessed prioritized PoC to highlight process gaps.
3. **Deliver**
   - Updated AI Triage, Risk Assessment, Inventory, and Governance Framework.
   - Delivered training, handover, and guidance to embed governance in 3LoD teams.
4. **Control**
   - Conducted technical and data science assessments.
   - Defined standards and frameworks to strengthen AI controls.

Impact

The initiative has transformed AI governance from a static framework into an operational model; scalable, compliant, and risk-aligned.

The company is now better equipped to deploy AI responsibly and ethically, while maintaining trust with regulators, stakeholders, and customers

Core principles

- Uplift, not recreate
- Keep it simple
- Comprehensive input
- Tailored to AI lifecycle stages
- Continuous improvement

CLIENT STORY 02 Ensuring safe, scalable rollout of GenAI program

Client challenge

A global energy and services group launched a program to accelerate GenAI adoption across its entities.

With 70+ projects since 2023, the organization faced rising risks from AI without centralized governance or consistent methodologies. Key challenges included:

- No unified AI risk framework
- Fragmented governance and tools
- Limited executive sponsorship
- Inconsistent cybersecurity and compliance
- Growing reliance on third-party AI providers

These gaps jeopardized safe, scalable GenAI deployment, especially for projects involving sensitive data and complex integrations. The company needed support to steer and assess cybersecurity, privacy, and legal risks across the program.

Approach

A tailored GenAI risk management methodology was developed, structured around three core areas:

1. Internal GenAI Risk Management

- Created **AI risk awareness deck** and early-stage **risk assessment questionnaire**.
- Designed **security reflex cards** for different AI system types.
- Implemented a **RACI matrix** to define stakeholder roles.

2. Third-Party Risk Management

- Built **pre-RFP and RFP questionnaires** to evaluate external AI providers.
- Aligned assessments with legal, privacy, & cybersecurity teams.

3. AI Governance and Policy

- Helped define a **group-level AI policy** and assessed 15+ use cases.
- Proposed governance models like centralized methodology and AI Hub.
- Ensured adaptability based on project sensitivity and data exposure.

Impact

The GenAI risk methodology delivered clear benefits:

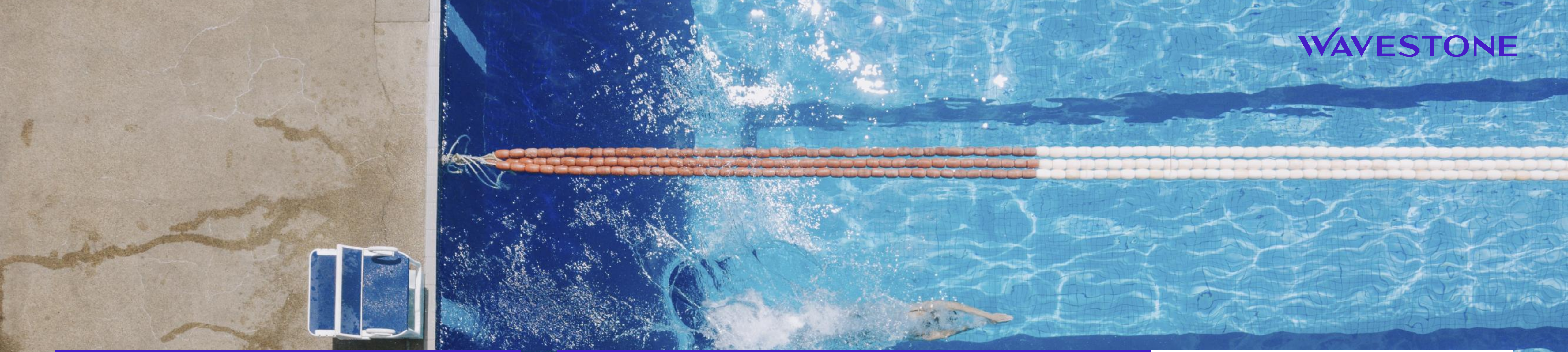
Better risk visibility: 15+ projects assessed, identifying limited-to-moderate risks and high-risk scenarios like data leaks and phishing.

Stronger alignment: RACI clarified accountability, improving execution and ownership.

Faster third-party checks: New questionnaires streamlined provider evaluations, reducing delays.

Scalable governance: Framework enables broader adoption and integration with cybersecurity processes.

Strategic readiness: Organization now proactively manages GenAI risks with robust tools and governance.



About Wavestone

Wavestone is your most trusted consulting partner for strategic transformations worldwide.

With a global presence, we stand by our clients in all regions as they develop solutions for an intensively competitive and fast-changing market.

Becoming more resilient and agile in a sustainable way, as technology, digitalization, and generative AI reshape industries and business operations: this is the incredible challenge we take on every day by your side.

How do we help clients with AI Governance and Risk Management?

Wavestone have extensive capabilities across AI, which can be leveraged to address AI challenges and develop holistic AI Governance.

Our core capabilities address AI Governance challenges comprehensively:

- Data Quality & Ethics
- Data Privacy and Protection
- Risk Management
- Cyber Security & Resilience
- Regulatory and Compliance
- Change Delivery

View more insights

- Article: The global AI regulations tracker
- AI in 2025: Current initiatives and challenges
- Guide: Implementations of the EU AI Act
- 2025 Data & AI Radar
- Client story: How did a global insurer strengthen their operational resilience?

Visit the Compliance section of our website

Authors

Mathew Wells

Associate Partner

Mathew helps organizations navigate and implement strategic operational and regulatory change in a complex and evolving environment. With over 15 years of experience in consulting and banking, he has deep expertise in operational risk and resilience, transformation, and operating model optimization.

Madeleine Thirsk

Senior Manager

Madeleine is a technology risk and controls expert at Wavestone, specializing in AI and IT risk management, governance, and compliance. She enables organizations to innovate securely by designing and optimizing resilient, risk-aligned solutions and control frameworks.

Contributors

Christian Brockhausen

Associate Partner

Gonzalo Cabrera Gonzalez

Senior Manager

AI Governance and Risk Management

Global experts

Wavestone has global expertise in AI governance and risk management.

Christine Kusztrich

Partner

Austria

Raimondo Costa

Partner

Switzerland

Ghislain De Pierrefeu

Partner

France

Jan-Hendrik Uhlenberg

Associate Partner

Germany

Romain Porot

Associate Partner

Switzerland

Julian Bischof

Associate Partner

Germany

WAVESTONE