MARSH & McLENNAN
ADVANTAGE

GOVERNING ARTIFICIAL INTELLIGENCE

Managing business risks in a digital world

Ben Hoster
Graeme Riddell
Richard Smith-Bingham

MARSH   GUY CARPENTER   MERCER   OLIVER WYMAN

INTRODUCTION

The explosion in the use of artificial intelligence (AI) by businesses over the past few years has driven an unmistakable inflection in corporate innovation, efficiency, and profitability. However, it has also exposed firms to ethical pitfalls and wasted investments, making effective governance and risk management vital.

A pervasive and critical element of corporate growth strategies, AI has fully extended its reach beyond the agendas of Big Tech and digital platform players. Predictably, companies are using AI-based solutions to augment critical business capabilities, such as advanced customer preference analytics, operational process optimization, cyber risk management, and customer and supplier engagement.[1] As the technology grows in sophistication and ubiquity, it becomes increasingly difficult both to monitor and understand how the algorithms derive outputs. This in turn presents challenges for anticipating downstream ramifications for a firm's business processes and the interconnections between these processes, partner companies, and society at large.

In the absence of appropriate risk management mechanisms, this opacity can expose businesses — and those individuals and communities dependent on them — to undesirable consequences. A poorly deployed AI solution may result in suboptimal decisions based upon flawed outputs and diminished returns on technology investments. Enduring reputational damage may arise from profit-driven overreach if businesses sell or otherwise capitalize on sensitive data and analytical or behavioral insights obtained in inappropriate ways.

Grappling with COVID-19 has also seen some organizations accelerate AI deployment to counter the impacts of the pandemic. Although valuable in supporting public health initiatives and improving efficiency, deployment without safeguards — especially at rapid speed — can expose organizations to risk (see sidebar: "*COVID-19 implications: accelerated AI deployment*").

Societal concerns have also emerged with regard to AI intruding on individual privacy, locking in systemic bias, and eroding social discourse. Lawmakers and regulators are being pressed to simultaneously keep pace with the impacts of a rapidly evolving technology while also addressing public concerns. Companies must therefore carefully navigate discontinuities across regulatory bodies as well as a diverse network of stakeholders in order to maintain their social license to employ AI capabilities.

Anticipating these growing business risks and external pressures, it is imperative that business leaders adopt effective governance practices. This requires a business-centric framework that is multifaceted and forward-looking, and one that addresses the diverse risks associated with the dynamic nature of AI technology. To that end, this paper sets out a five-dimensional governance framework, along with guidance on implementation practices.

[1] Forbes. (2020). Roundup of Machine Learning Forecasts and Market Estimates, 2020. Retrieved October 12, 2020, from https://www.forbes.com/sites/louiscolumbus/2019/03/27/roundup-of-machine-learning-forecasts-and-market-estimates-2019/#29b08337695a

COVID-19 implications: accelerated AI deployment

The COVID-19 pandemic is accelerating the scale and usage of AI technology as governments and businesses alike respond to this unprecedented crisis.

AI is touted as a pandemic super tool that can profile infection risk, triage chest scans, catalyze vaccine development, and generally bolster response efforts to enhance contact tracing, facilitate social distancing, and more. It also has the potential to support economic recovery. Digital health surveillance tools can be pivotal in helping businesses facilitate a safe return to the workplace.[2]

Moreover, social distancing practices are leading businesses to introduce automated solutions for predicting consumer behavior, optimizing supply chains, and improving delivery efficiency. Research suggests that perhaps 40 percent of companies worldwide are increasing their use of workplace automation in response to the pandemic.[3]

The use cases for AI deployment can also make the balancing of risks and trade-offs a more acute challenge. Surveillance technologies such as facial recognition, contact tracing, and AI-enhanced infection risk profiling require both businesses and governments to weigh the dual imperatives of public health and individual liberty. Additionally, businesses deploying automation technology to maintain output with fewer workers and reduce the risk of COVID-19 outbreaks in the workplace may find themselves in the spotlight for exacerbating societal inequality and unemployment.

[2] Marsh & McLennan Advantage. (2020). Digital Health Surveillance — A Balancing Act for Business. https://www.mmc.com/content/dam/mmc-web/insights/publications/2020/august/Digital-Health-Surveillance_Final.pdf

[3] Wall Street Journal. (2020). Tech Workers Fear Their Jobs Will Be Automated in Wake of Coronavirus. Retrieved October 12, 2020, from https://www.wsj.com/articles/tech-workers-fear-their-jobs-will-be-automated-in-wake-of-coronavirus-11590571801

INTRINSIC RISKS IN AI TECHNOLOGY DEPLOYMENT

Businesses will be exposed to near-term financial and enduring reputational harm if they do not exhaustively identify and address the risks associated with the establishment and operation of AI-based applications.

While the risks associated with the use of AI applications loom large, they are generally able to be mitigated by organizations using those technologies, if they are properly identified and managed through an effective governance framework (see Exhibit 1).

IDENTIFYING NEAR-TERM FINANCIAL RISKS

Existing IT governance practices in many firms will help ensure the effective development and delivery of AI technologies. But they are typically not suited to foreseeing or addressing the potential for unexpected adverse outcomes.

These eventualities often occur due to the very nature of AI technology. Even simple rules and inputs — when implemented with self-learning, automated, algorithmic engines — can create outputs that are difficult to predict and therefore manage. Undetected errors in AI deployment or subsequent model drift could also affect other areas of an organization and create the possibility of positive feedback loops wherein detrimental outcomes become amplified over time and not detected until too late.

Exhibit 1: Intrinsic risks associated with the use of AI

Near-term financial risks

- Ineffective governance leads to misallocated investments, magnified risks, and limited gains
- Inability to explain adverse outcomes produced by "black box" AI systems harms credibility, consumer and stakeholder trust, and thus revenue
- Cyberattacks through direct and indirect AI output manipulation destabilize AI systems

Enduring reputational risks

- Profit-driven overreach from information misuse tarnishes the corporate brand and creates legal risk
- Limited training data diversity and homogeneous development teams lead to biased outputs
- Automation exacerbates unemployment and social inequality, creating public dissent

Source: Marsh & McLennan Advantage

Businesses are also susceptible when they use "black box" AI systems with minimal transparency or traceability. Unexplainable algorithms pose a risk that is particularly pertinent for firms that adopt AI solutions from external vendors or apply them in important decision-making processes such as credit-risk assessments and medical diagnoses. Especially when adverse outcomes to customers and staff are possible, firms must be able to explain and defend algorithm-based decision processes and their output to a range of stakeholders, including subject-matter experts and even the legal community in cases of alleged malpractice.

Due to increasing reliance on technology networks, AI-enabled cyberattacks also present an attractive threat vector and tool for cybercriminals. Given the rapidity with which AI applications make decisions, bad actors can cause disproportionate harm once they have infiltrated AI programs, maliciously tweaking input parameters or discrete lines of code, which may not be detected without proper checks and balances.[4] Moreover, the automated discovery and exploitation of cyber vulnerabilities through spear-phishing is now a "smarter" and more dangerous means of gaining access to sensitive systems and pilfering confidential information.[5] These attacks may destabilize firms' digital capabilities, disrupting their operations and revenue generation.

Certain business applications of AI technology may directly affect various groups within society, leading to reputational harm and revenue erosion

UNDERSTANDING ENDURING REPUTATIONAL RISKS

Certain business applications of AI technology may also directly affect various groups within society, leading to reputational harm and revenue erosion.

Profit-motivated overreach has exposed organizations to the risk of litigation and reputational impairment, such as when they use the personally identifiable information (PII) of citizens for purposes beyond those originally sanctioned. Companies may be tempted to find novel ways of monetizing consumer data — powering recommendation engines to steer unwitting consumers or harvesting and selling personal information to third parties — where limits on collection, processing, and distribution are not clearly defined. Other forms of overreach are also growing in frequency, such as the unauthorized surveillance of consumers or the exploitation of personal data to influence political processes.

AI applications can also inadvertently generate biased and potentially discriminatory outputs when the dataset used to "teach" an algorithm is insufficiently expansive. As is well known, even dominant data accumulators have been caught off-guard, such as when internal recruiting applications deprioritized female or ethnic minority candidates or when chatbots used racist and anti-Semitic language.[6] This is exacerbated when historical data is used for training, codifying and consolidating the systemic inequalities and discrimination that may subconsciously exist within societies and organizations. Biased training data is not the only issue: product teams — often predominantly male and white — can unintentionally perpetuate prejudice when their demographic homogeneity predisposes them to be unaware of divisive societal fault lines.[7]

[4] TechGenix. (2019). AI cyber risks: What to look out for when deploying AI technology. Retrieved October 12, 2020, from http://techgenix.com/ai-cyber-risks/

[5] United Nations Interregional Crime and Justice Research Institute. (2019). Artificial Intelligence and Robotics for Law Enforcement. Retrieved October 12, 2020, from http://www.unicri.it/news/article/Artificial_Intelligence_Robotics_Report

[6] Reuters. (2018). Amazon scraps secret AI recruiting tool that showed bias against women. Retrieved October 12, 2020, from https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

[7] The Guardian. (2019, April 17). Disastrous lack of diversity in AI industry perpetuates bias, study finds. Retrieved October 12, 2020, from https://www.theguardian.com/technology/2019/apr/16/artificial-intelligence-lack-diversity-new-york-university-study

EXTERNAL PRESSURES FROM THE BROADER PUBLIC AGENDA

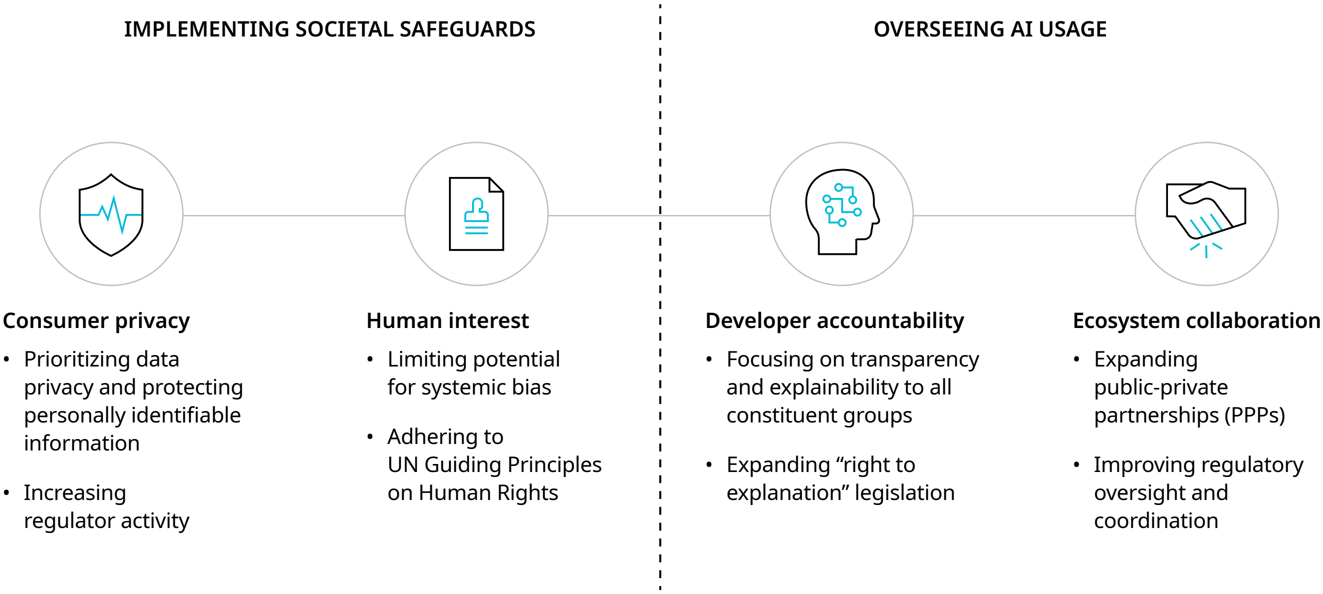
Businesses face external constraints as policymakers, regulators, and societies collectively work towards norms that balance private entrepreneurialism with public interest, instituting policies that govern the application of AI technology and sometimes herald long-term, often opaque, societal consequences.

Firms should be attuned to how policymakers and the public AI governance agenda may shape the business landscape in which organizations that leverage AI technology operate (see Exhibit 2).

IMPLEMENTING SOCIETAL SAFEGUARDS TO PROTECT THE PUBLIC INTEREST

Since AI algorithm inputs often include PII, consumers will predictably be exposed to new, powerful, and potentially meddlesome uses of their data.

Exhibit 2: Public governance agenda overview



IMPLEMENTING SOCIETAL SAFEGUARDS

Consumer privacy

- Prioritizing data privacy and protecting personally identifiable information
- Increasing regulator activity

Human interest

- Limiting potential for systemic bias
- Adhering to UN Guiding Principles on Human Rights

OVERSEEING AI USAGE

Developer accountability

- Focusing on transparency and explainability to all constituent groups
- Expanding "right to explanation" legislation

Ecosystem collaboration

- Expanding public-private partnerships (PPPs)
- Improving regulatory oversight and coordination

Source: Marsh & McLennan Advantage

In widely disseminated press reports, some technology companies were much criticized over the alleged misuse of sensitive voice data recorded by their AI-powered digital assistants. In response, two US states enacted data privacy laws in 2018, and more than 17 others have since passed or drafted similar bills.[8] Given firms' enduring ability to generate insights from big data and subsequently exploit personal profiles in ways that consumers have not anticipated or accepted,[9] such scrutiny will surely persist.

In response to public concern about systemic bias in algorithm-based decision-making and also the potential for machines to usurp jobs, civil society organizations are calling on the business world to use AI in accordance with the UN Guiding Principles on Human Rights.[10] This might directly affect firms' bottom lines. Recent instances show users and, importantly, advertisers boycotting platforms, as well as employees advocating for change in sales practices.

Expanding the use of "right to explanation" laws is also being used in several US states to increase transparency in AI applications. Companies are quickly recognizing the importance of accountability in gaining and retaining public trust: many leading companies are already actively pledging to be transparent of their own accord.[11] However, while firms must be proactive in meeting these expectations, to balance risks, they should also be selective in what is disclosed. In some instances, algorithms can be reconstructed and intellectual property subsequently stolen based solely on the explanation of their output.[12]

OVERSEEING AI USAGE IN AN EVOLVING BUSINESS LANDSCAPE

As their use of AI solutions grows, businesses would benefit from taking soundings from a more expansive network. This might range from engaging with local academic institutions on the one hand to more formal public-private partnerships (PPPs) on the other. For instance, the National Science Foundation and the Partnership on AI, a network of more than 100 partners across 13 countries, is currently researching the sociotechnical dimensions of AI use.[13]

Since AI algorithm inputs often include PII, consumers will predictably be exposed to new, powerful, and potentially meddlesome uses of their data.

[8] Virtu. (2020). Infographic: Data Privacy Law Momentum at the State Level. Retrieved October 12, 2020, https://www.virtru.com/education/data-privacy-law-infographic/

[9] CNET. (2019). Amazon and Google are listening to you: Everything we know. Retrieved October 12, 2020, https://www.cnet.com/how-to/amazon-and-google-are-listening-to-your-voice-recordings-heres-what-we-know/

[10] Global Future Council on Human Rights 2016-2018. (2018). How to Prevent Discriminatory Outcomes in Machine Learning. World Economic Forum. http://www3.weforum.org/docs/WEF_40065_White_Paper_How_to_Prevent_Discriminatory_Outcomes_in_Machine_Learning.pdf

[11] IBM. (2019). IBM'S Principles for Data Trust and Transparency. Retrieved October 12, 2020, https://www.ibm.com/blogs/policy/trust-principles/

[12] Milli, S., Schmidt, L., Dragan, A. D., & Hardt, M. (2019). Model reconstruction from model explanations. In Proceedings of the Conference on Fairness, Accountability, and Transparency (pp. 1-9). https://dl.acm.org/doi/abs/10.1145/3287560.3287562?download=true

[13] Select Committee on Artificial Intelligence of the National Science and Technology Council. (2019). The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update. https://www.whitehouse.gov/wp-content/uploads/2019/06/National-AI-Research-and-Development-Strategic-Plan-2019-Update-June-2019.pdf

Beyond allowing public and private sectors to share best practices for public benefit, partnership projects and networks can generate long-term advantages for companies. These include brand enhancement with customers, new commercial opportunities with different partners, and a stronger voice in policy debates. Trust and transparency regarding data ownership and access on co-developed AI platforms is critical for success, especially when these platforms operate in the public domain, such as Smart City arrangements. AI can be a tool for enhancing value but also for obscuring how data is used — and by whom — if its use is not governed by appropriate controls.

The complexity of operating within this network is compounded by the global fragmentation of data standards, which continues to impede the effectiveness of regionally focused regulatory efforts. The General Data Protection Regulation (GDPR), for example, cannot prevent personal information that was "forgotten" in the EU domain from being displayed in AI-enabled search engines outside of the region.[14] Companies operating across jurisdictions may struggle to align their usage of AI with regional mandates necessitating decentralized policy rollouts tailored to specific contexts and geographies. Furthermore, companies with one value system may struggle against competitors operating in accordance with different principles.

Companies with one value system may struggle against competitors operating in accordance with different principles.

[14] Towards Data Science, Medium. (2019). Looking at AI-focused Case Studies. Retrieved October 12, 2020, https://towardsdatascience.com/looking-at-ai-focused-case-studies-139e0bb98ff5

AI GOVERNANCE

To mitigate risks and realize the potential of AI, businesses need a governance framework that is based on intent, fairness, transparency, safety, and accountability. To operationalize it effectively, they must then establish adequate safeguards, ensure active oversight arrangements, and institute an internal process for maintaining control.

TOWARDS RESPONSIBLE AI DEPLOYMENT AND USE

Growing awareness of the pitfalls and societal impacts of AI use has sparked an explosion of AI governance frameworks (see sidebar: "*A review of published AI governance frameworks*"). An assessment of more than 60 publications against the intrinsic risks and external pressures set out above suggests that businesses should base their AI governance efforts across five critical dimensions:

INTENT: By using data in a principled manner and verifying that AI design and implementation processes are ethically aligned and appropriate, businesses will be better positioned to manage risks and execute their internal review and oversight processes.

FAIRNESS: Companies need to ensure that the processes and outputs of their AI system do not unwittingly discriminate against any group or individual. By achieving this, firms can reap reputational benefits, foster greater public trust, and minimize the external risks to their business.

TRANSPARENCY: Companies should ensure that their AI processes are explainable and repeatable. Not only does this facilitate compliance reviews and stakeholder trust, it also supports continued efforts to improve AI development and deployment.

SAFETY/SECURITY: Companies that establish robust capabilities in data governance, threat protection, and user privacy are better able to detect malicious incursions, thereby mitigating adverse outcomes, minimizing their legal liability, and maximizing the utility of their data.

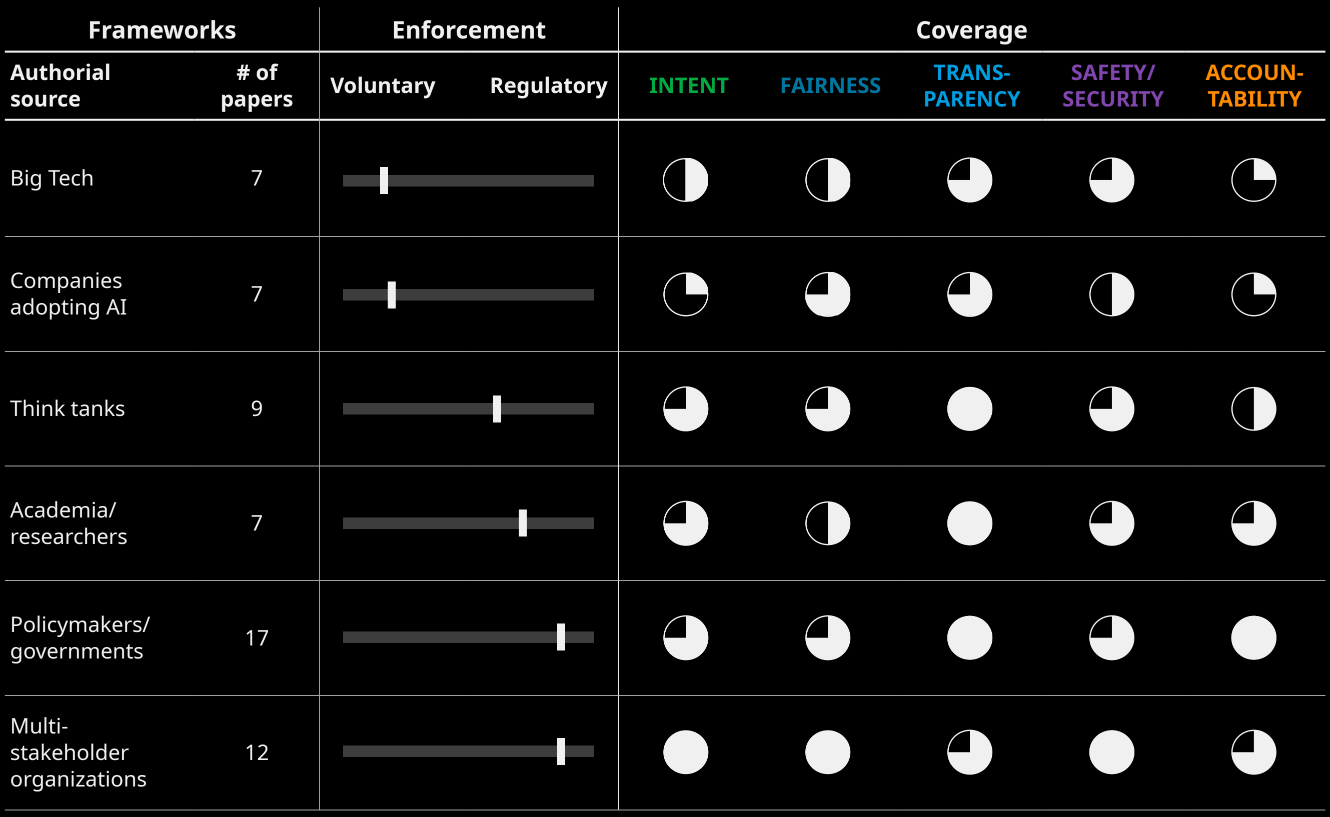
ACCOUNTABILITY: Companies should undertake rigorous audit and compliance assurance processes. Those that are mindful of the concerns of their various stakeholders — lawmakers, auditors, customers, business partners, and shareholders, among others — will better build confidence, fulfill regulatory requirements, and avoid complications in the future.

A review of published AI governance frameworks

A review of 60-plus published frameworks highlights how different types of author place a different value on each dimension and how they should be enforced (see Exhibit 3).

Frameworks published by companies, both Big Tech and those adopting AI, tend to focus on voluntary best-practice mechanisms rather than regulation. Additionally, they are less vocal than other types of authors with regard to Accountability and Intent — in comparison to Transparency and Safety/Security. This instinctive reticence may expose them to consumer and regulatory backlash in the event of things going wrong.

Exhibit 3: Summary of governance frameworks



Frameworks		Enforcement		Coverage				
Authorial source	# of papers	Voluntary	Regulatory	INTENT	FAIRNESS	TRANS-PARENCY	SAFETY/ SECURITY	ACCOUN-TABILITY
Big Tech	7	──▮────────		◑	◑	◕	◕	◔
Companies adopting AI	7	──▮────────		◔	◕	◕	◑	◔
Think tanks	9	──────▮────		◕	◕	●	◕	◑
Academia/ researchers	7	───────▮───		◕	◑	●	◕	◕
Policymakers/ governments	17	────────▮──		◕	◕	●	◕	●
Multi-stakeholder organizations	12	────────▮──		●	●	◕	●	◕

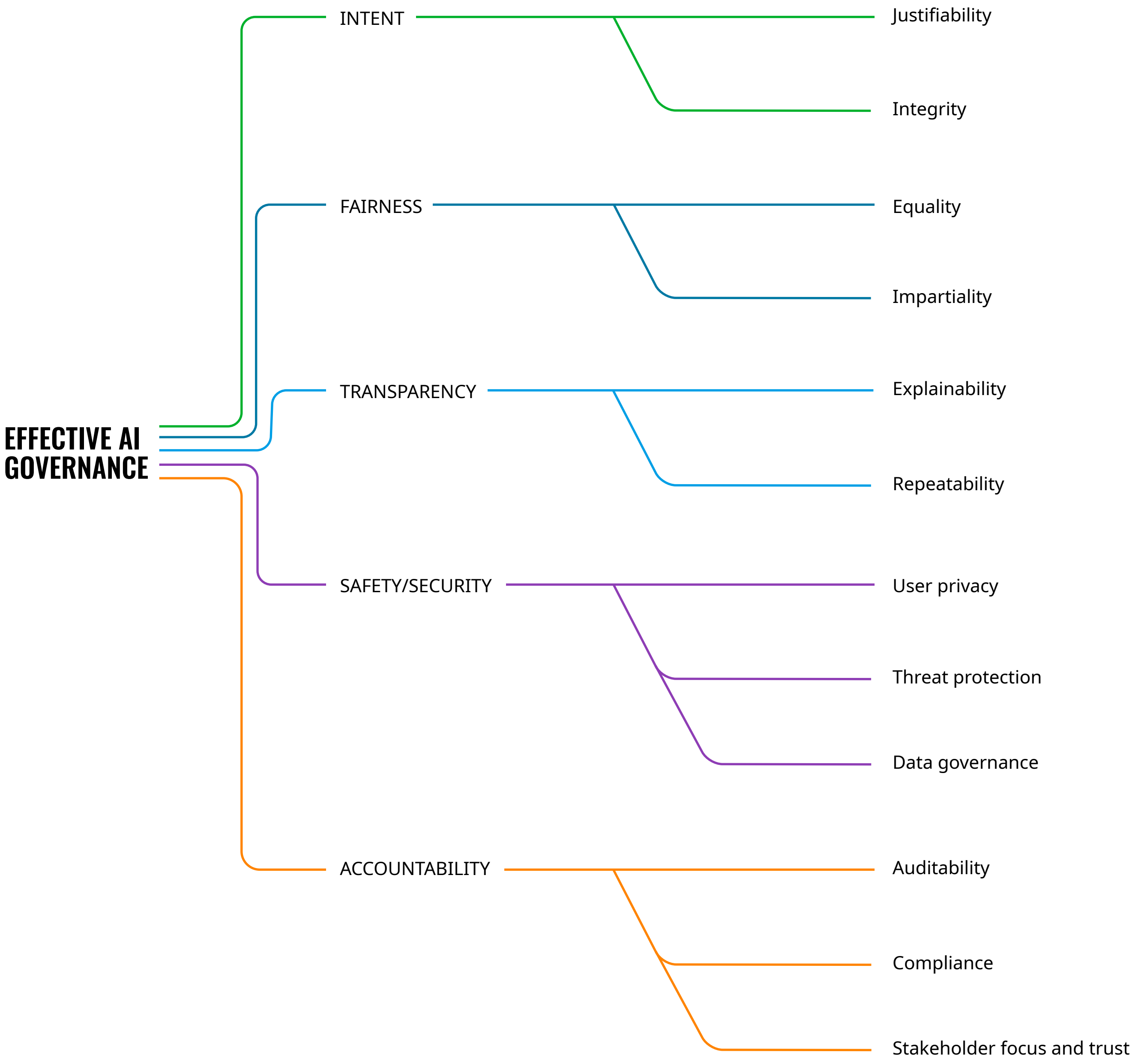
Topical focus:

● Very prevalent, frequently addressed ○ Less prevalent, occasionally considered

Source: Marsh & McLennan Advantage

The following framework expands on the five dimensions to help firms effectively oversee and assess their usage of AI technology (see Exhibit 4).

Exhibit 4: A holistic approach to effective governance



Source: Marsh & McLennan Advantage

	Imperative	Why it matters
INTENT	**Justifiability** Demonstrate that design and implementation processes, as well as the decision output, are aligned with expressed purpose	• Provides assurance that decisions adhere to intended objectives and logic • Facilitates internal review and oversight • Enhances risk management for new and existing models
	Integrity Ensure data is used in a responsible and appropriate manner	• Prevents negative social outcomes and brand implications associated with improper harvesting and selling of data
FAIRNESS	**Equality** Promote equal access and similar opportunities for all individuals and groups	• Mitigates the risk of disenfranchisement • Fosters public trust • Contributes to alleviating broader societal inequality
	Impartiality Minimize the likelihood/occurrence of biased outcomes	• Protects brand by mitigating algorithmic bias through internal and external oversight mechanisms
TRANSPARENCY	**Explainability** Produce explanatory diagnostics — inputs, intermediate factors, and outputs — that can be interpreted by developers, practitioners, and consumers; eliminate “black box” outputs	• Enables continued improvement efforts • Facilitates internal compliance reviews • Builds consumer confidence and accelerates adoption
	Repeatability Generate predictable and reproducible outputs complemented by effective supervision and maintenance processes	• Builds confidence in model output and reliability • Overcomes inherent trust issues and facilitates stakeholder acceptance
SAFETY/SECURITY	**User privacy** Protect consumer privacy and restrict AI influence to the express purpose for which it is intended	• Safeguards customer rights and builds trust and reputation • Minimizes legal liability
	Threat protection Guard AI decision engines from overt intrusion and indirect malicious inputs	• Prevents unintended algorithmic outputs • Builds user confidence in the system’s ability to safely function as intended
	Data governance Manage data assets in a holistic fashion to generate value from information	• Ensures data accessibility, usability, integrity, and security • Maximizes utility of data
ACCOUNTABILITY	**Auditability** Provide traceable and verifiable model outputs that can be tested both internally and externally, with simulated or real data inputs	• Enables model assessment for bias, compliance, accuracy • Produces auditable system records — inputs, logic, outputs — to ensure adherence to auditing standards/criteria
	Compliance Adhere to relevant laws and contribute to regulatory agenda	• Fulfills ethical compliance standards • Allows the business and industry to play a role in shaping the AI regulatory agenda
	Stakeholder focus and trust Implement stakeholder-centered policies with clear enforcement mechanisms	• Prioritizes the collective benefit of all stakeholders — customers, shareholders, employees, partners, etc. • Requires a higher duty of care and disclosure to prevent improper outcomes — data expiration/use, facial recognition stipulations, etc.

ACTIVATING GOVERNANCE

A framework is only useful if it can be practically and effectively implemented. In applying it, companies need to institute supporting governance infrastructure and mechanisms — an oversight committee, risk register, testing, and policy development and enforcement, among others — in a structured and rigorous manner (see Exhibit 5). With proper oversight in place, concerns can be identified and mitigation initiatives pursued.

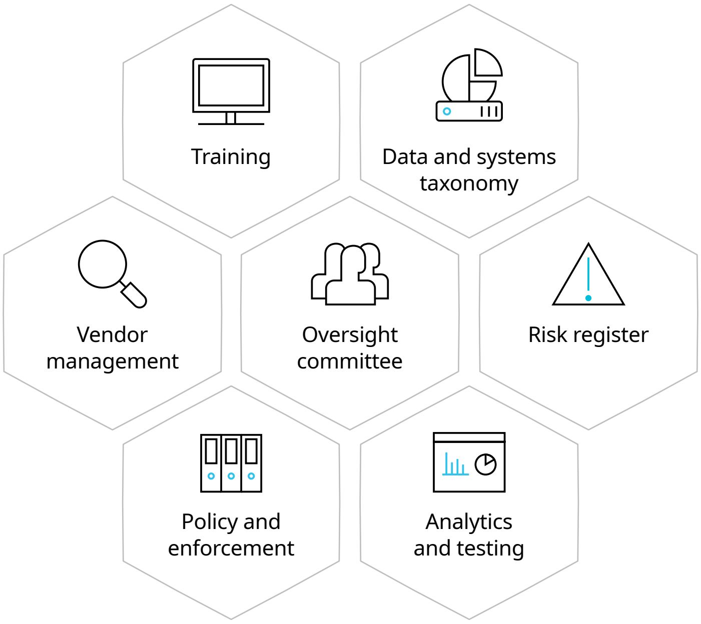
An **oversight committee**, independent of the development team and with a level of ambition endorsed by the Board of Directors, should be convened to ensure AI technologies are deployed in alignment with the firm's values and monitored to ensure adherence to control arrangements. It may be useful for this committee to comprise senior representatives from key functions such as risk management, IT, public affairs, legal, compliance, audit, and human resources to ensure a range of perspectives. The committee will also need to determine the value of, and approach to, decentralizing subsequent tiers of oversight.

To enable comprehensive coverage and oversight, a **data and systems taxonomy** should be established to serve as a guide, which details specific AI applications (including third-party solutions): This would capture data inputs and usage patterns, any associated sensitivities, required validation and testing cycles, and expected outputs.

A **risk register** should then set out the types of issues that may arise, linking this to systems and risk sources. This can be a foundation for appreciating the magnitude of the impact, the level of vulnerability, and the extent of the control regime and monitoring protocols to be applied.

Analytics and testing should be executed on a frequent and ongoing basis to monitor those risk issues that relate to system inputs, outputs, and model components. Such elements might include explainability features, bias checks, consistency monitors, intervention thresholds, back testing, and validation.

Exhibit 5: Elements of disciplined governance



Source: Marsh & McLennan Advantage

Policies and enforcement should establish norms, roles and accountabilities, approval processes, maintenance guidelines, and change control across the development lifecycle — from initiation to decommissioning. Key performance indicators, based on clear standards and tolerances, can be used to monitor compliance and measure improvement.

When using third-party solutions, it is critical to have proper **vendor management** practices and understand the robustness of vendor controls, with appropriate transparency on deviations enshrined in contracts.

Training and awareness programs for staff involved in developing, selecting, or using AI tools should be mandatory to ensure behaviors and processes are aligned with corporate expectations.

Where AI use is under particular public scrutiny, or businesses are otherwise trying to strengthen stakeholder trust, it may benefit companies to bring in independent and reputed third parties. Such parties would obviously need sufficient access and authority to effectively highlight gaps and recommend meaningful corrective actions if the business is to avoid the perception of a whitewashing.

Critically, governance mechanisms and companies must place a focus on continuous review and improvement — both at an AI application level via systems testing to mitigate potential lapses if model drift occurs and the algorithm requires recalibration and testing, and also at the process level to account for technological developments that may require revisions to wholesale testing strategies, training and awareness programs, or oversight arrangements. Businesses that elect to use external AI solutions should not assume that the vendor will bear the brunt of any mishap. The customer’s first inclination is to hold the most proximal source of the overstep accountable.

AI has the potential to bring significant efficiencies and unlock new potential for business by automating processes and identifying hidden opportunities through analytical insights. However, realizing this is only possible if risks are managed. By framing the governance of their AI solutions around the five dimensions identified and instituting the governance processes outlined, businesses can ensure that they do not expose themselves to undue risk, or worse, inadvertently cause harm to broader society.

ABOUT MARSH & MCLENNAN COMPANIES (MMC)

Marsh & McLennan (NYSE: MMC) is the world's leading professional services firm in the areas of risk, strategy and people. The Company's 76,000 colleagues advise clients in over 130 countries. With annual revenue of $17 billion, Marsh & McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses. Marsh advises individual and commercial clients of all sizes on insurance broking and innovative risk management solutions. Guy Carpenter develops advanced risk, reinsurance and capital strategies that help clients grow profitably and pursue emerging opportunities. Mercer delivers advice and technology-driven solutions that help organizations redefine the world of work, reshape retirement and investment outcomes, and unlock health and wellbeing for a changing workforce. Oliver Wyman serves as a critical strategic, economic and brand advisor to private sector and governmental clients.

For more information, visit www.mmc.com, follow us on LinkedIn and Twitter @mmc_global or subscribe to BRINK.

AUTHORS

Ben Hoster

Director,
Marsh & McLennan Advantage

Graeme Riddell

Research Manager,
Marsh & McLennan Advantage

Richard Smith-Bingham

Executive Director,
Marsh & McLennan Advantage

Special recognition is extended to Rachel Lam for her diligent assistance in developing the AI governance framework.

CONTRIBUTORS

Leslie Chacko, Darrel Chang, Ege Gurdeniz, Usha Jagannathan, Spencer Long, Kiran Mudiam, Elizabeth St-Onge, Asha Vellaikal

This report and any recommendations, analysis or advice provided herein (i) are based on our experience as insurance and reinsurance brokers or as consultants, as applicable, (ii) are not intended to be taken as advice or recommendations regarding any individual situation, (iii) should not be relied upon as investment, tax, accounting, actuarial, regulatory or legal advice regarding any individual situation or as a substitute for consultation with professional consultants or accountants or with professional tax, legal, actuarial or financial advisors, and (iv) do not provide an opinion regarding the fairness of any transaction to any party. The opinions expressed herein are valid only for the purpose stated herein and as of the date hereof. We are not responsible for the consequences of any unauthorized use of this report. Its content may not be modified or incorporated into or used in other material, or sold or otherwise provided, in whole or in part, to any other person or entity, without our written permission. No obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof. Information furnished by others, as well as public information and industry and statistical data, upon which all or portions of this report may be based, are believed to be reliable but have not been verified. Any modeling, analytics or projections are subject to inherent uncertainty, and any opinions, recommendations, analysis or advice provided herein could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. We have used what we believe are reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied, and we disclaim any responsibility for such information or analysis or to update the information or analysis in this report.

We accept no liability for any loss arising from any action taken or refrained from, or any decision made, as a result of or reliance upon anything contained in this report or any reports or sources of information referred to herein, or for actual results or future events or any damages of any kind, including without limitation direct, indirect, consequential, exemplary, special or other damages, even if advised of the possibility of such damages. This report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. No responsibility is taken for changes in market conditions or laws or regulations which occur subsequent to the date hereof.