ISACA

Artificial Intelligence Governance Brief

Summary

Artificial intelligence (AI) is a proliferating technology with unique benefits and risk. Are organizations prepared to use it? Are they in a position to govern and manage its use? Does governance over AI facilitate and promote the organization's strategic direction and create value? These questions are explored in this governance brief, and a questionnaire is provided to help organizations self-assess their AI governance systems.

The emergence of AI is a significant opportunity that brings with it both strategic and operational risk. AI is not something that can be ignored. As AI maturity grows, enterprise customers will demand its benefits. Staff will use available AI tools whether the organization has a strategy or not, incurring the associated risk. For this reason, governing bodies should set the strategic approach for AI while ensuring that there are clear boundaries for its use.

AI integration and adoption can be achieved through the purchase of commercial off-the-shelf AI software or software developed in-house and then implemented by leveraging a cloud provider or on-premises environment. Unplanned AI adoption can occur in an enterprise with little to no oversight, particularly given the availability of AI solutions included in products already in use. It is essential that governing bodies are positioned to demonstrate proper stewardship over this technology and exhibit robust governance and ethical practices that mitigate the risk of harm and help ensure AI accountability, transparency, and fairness.

AI Benefits

The use of AI in an organization can drive efficiency, innovation, competitive advantage, and long-term value creation. Important AI benefits for an enterprise include:

Increased Innovation—AI can enable innovation, helping organizations develop unique products, services, or business models that differentiate them from competitors and give them an edge in the market.

Enriched Data Analysis—AI can be used to analyze vast amounts of data in real time, which enables organizations to base their strategic decisions on more accurate and actionable insights, leading to better alignment with market trends and customer needs.

Improved Customer Service—AI can be used to personalize customer interactions and automate service delivery. This can strengthen customer loyalty and satisfaction, a key driver of sustainable growth.

Automation—AI can be used to automate processes and improve delivery efficiency. It can help enterprises reduce operations costs, enabling them to focus resources on innovation and strategic initiatives.

Enhanced and Continuous Monitoring—AI can enhance an organization's ability to monitor and mitigate risk, ensuring compliance with regulatory requirements and improving governance processes.

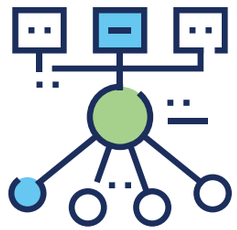
The challenge for governing bodies and executive management is that achieving such benefits goes beyond technological adoption to involve redesigning key business processes and potentially even developing new business models.

AI Risk

The rapid development and widespread use of AI offers many benefits, but it also poses significant risk to organizations and society. This risk spans across ethical, technical, legal, and societal domains. Some of the most critical risks to consider include:

Bias and discrimination as a result of biased training data

Ethical dilemmas



Manipulation through poorly designed algorithms

Lack of transparency due to opaque algorithms

Lack of accountability through autonomously operated AI systems

Security and privacy risk and potential AI weaponization

Compliance risk through increased regulations and/or regulatory ambiguity

User and Provider Roles

An organization can assume different roles when it comes to AI. Almost every organization takes the role of a “user” in some way or another (knowingly or not), as many types of software and services utilize AI. Organizations can also integrate AI into their internal business processes or the services and products they deliver to their clients, effectively making them a “provider” of AI. In both cases, the questions and the key points of AI governance remain valid.

Questions to Consider

Governing bodies should ask themselves a series of questions about AI usage, and management and supporting functions should consider the responses and initiate actions, if necessary. Key AI benefit, risk, and resource questions are outlined in **figure 1**.

FIGURE 1: Key AI Benefits, Risk, and Resources

	TOPIC	QUESTIONS TO ASK
AI BENEFITS	Performance and Return on Investment (ROI)	How is the organization measuring the success and ROI of AI initiatives? Are AI investments delivering the expected business value?
	Business Alignment	Has consideration been given to how AI initiatives may support the organization's long-term strategic objectives?
	Organizational Readiness	Is the organization culturally and operationally ready for AI adoption? Does the organization have the right talent and change management strategies in place?
	Organizational Mission	What are the organizational needs, and how does AI align with the organization's vision?
	Value Creation	What are the benefits for the organization's products and services, operations and management, and stakeholders?
	Performance Management	Are the organization's AI benefit predictions realistic, and how are they tracked?
	Cost/Benefit Analysis	How are the benefits aligned with the organizational objectives and realized, measured, and monitored?
AI RISK	Risk Management	What risk is associated with AI deployment? How is the organization managing ethical, security, and reputational risk effectively? Is AI risk integrated into the enterprise risk register and risk governance process, and is it consistent with the corporate culture? Has AI risk to the organization's vision and stakeholders been evaluated?
	Regulatory Compliance	Is the organization keeping up with evolving AI regulations? Are measures in place to ensure ongoing legal and regulatory compliance? Is the organization aware of constraints, compliance requirements, and the potential negative impact of AI?
	Ethical AI Use	Are there frameworks in place to ensure AI systems operate ethically, with fairness, transparency, and accountability?
	Data Privacy and Security	Are there adequate processes to safeguard sensitive data accessed in AI systems (including confidential external and internal data)?
	Bias Mitigation	What steps are being taken to identify, mitigate, and prevent bias in AI systems to ensure fair and nondiscriminatory outcomes?
	Legal and Contractual	What is the impact on contractual agreements and legal obligations?
	Framework Adoption	Does an AI governance framework exist, and has it been adopted by the organization?
AI RESOURCES	Finance Involvement	Has the organization defined and allocated the right level of people, time, and budget for AI?
	Project Planning	Is there a clear overview of resource usage and outcomes?
	Human Resources	Have guidance, guardrails, appropriately skilled staff, and (third-party) resources been provided?
	Training And Education	Has the organization developed the right skills, resources, and platforms to ensure long-term value delivery and independence from third parties, where feasible?
	Communication Plans and Reporting	Have key performance indicators (KPIs) been defined and monitored by the organization?

Relevant Governance Components

The previous sections discussed the potential benefits and risk that must be considered for AI governance. Appropriate and adequate governance systems need to be defined to address these issues and answer the relevant governance-related questions. Key aspects of a defined governance system include the following components:

- A mature process for **information and technology (I&T) governance**, which ensures that stakeholder needs, conditions, and options are evaluated to determine balanced, agreed-upon enterprise objectives to be achieved; the direction is set through prioritization and decision making; and performance and compliance are monitored against the agreed-upon direction and objectives
- Mature processes for **innovation management, portfolio management, and external compliance management**
- Appropriate **governance structures**, e.g., a governance committee, board of directors, IT investment committee, risk committee, audit committee, and IT strategy committee
- The **skillset to make informed decisions on AI**, including a basic understanding of the technology and its implications (which can be accomplished through having members with sufficient AI knowledge and/or running awareness and training for members until the governing body has the minimum understanding of AI)

Existing governance and management systems need to be reviewed to ensure they are fit for purpose before AI is introduced. While the ultimate responsibility for AI rests with the governing body, it is important that:

- Committee charters are reviewed to ensure that AI-related issues are addressed in a timely manner.
- There is clear accountability for AI decision making between committees, management, and individuals.
- Safe and responsible AI principles are incorporated into relevant policies (e.g., AI/IT use, privacy, confidentiality, and cybersecurity).

For more on good practices for governance system components, refer to the COBIT® Framework, the most practical and comprehensive framework for I&T governance.

Visit www.isaca.org/ai for more AI resources, including guidance, policy templates and training.

AI Governance Questionnaire

The following interactive questionnaire (**figure 2**) can assist in determining the fitness of an organization's governance systems for AI.

FIGURE 2: AI Governance Questionnaire

		FULLY	LARGELY	PARTIALLY	NOT	UNKNOWN
1.	To what extent does the use of AI in organizational processes align with our values and vision?	☐	☐	☐	☐	☐
2.	Have the intended benefits been identified, and are these quantified on an ongoing basis for adequate business cases?	☐	☐	☐	☐	☐
3.	Which metrics will be used to measure the intended benefits of the use of AI?	☐	☐	☐	☐	☐
4.	Does the organization have a process in place to monitor the achievement of the intended benefits of the use of AI (e.g., the use of open-source AI to accrue and protect long-term value)?	☐	☐	☐	☐	☐
5.	Has the organizational risk associated with the use of AI been identified?	☐	☐	☐	☐	☐
6.	Has the organizational risk associated with the use of AI been quantitatively assessed?	☐	☐	☐	☐	☐
7.	Has a risk response been defined for each assessed risk (Note: 'accept' is a valid response)?	☐	☐	☐	☐	☐
8.	Does the organization have the required internal and external resources for developing and deploying AI capabilities?	☐	☐	☐	☐	☐
9.	Has the organization established a crossfunctional AI governing body/steering committee?	☐	☐	☐	☐	☐
10.	Has guidance from the governing body/steering committee been provided to the organization on the potential benefits and necessary boundaries of the use of AI?	☐	☐	☐	☐	☐
11.	Is monitoring in place to ensure compliance with relevant laws and regulations?	☐	☐	☐	☐	☐

Definitions

Artificial intelligence (AI)

An advanced computer system that can simulate human capabilities, such as analysis, based on a predetermined set of rules

Governing bodies

Includes the executive and nonexecutive directors or board and supervisory board

Management and supporting functions

Refers to roles such as C-suite, audit, legal, company secretary, risk, or security

Governance

Involves evaluation, direction, and monitoring

Value creation

The main governance objective of an enterprise, achieved when the three underlying objectives (benefits realization, risk optimization and resource optimization) are all balanced

Benefits

An outcome whose nature and value (expressed in various ways) are considered advantageous by an enterprise

Stakeholders

Includes shareholders, business partners (customers and suppliers), employees, authorities, and other groups with or without affiliation

Acknowledgments

ISACA 2024 Governance Advisory Group

J. Winston Hayden
CISA, CISM, CGEIT, CRISC, CDPSE
South Africa

Jimmy Heschl
CISA, CISM, CGEIT
Red Bull GmbH, Austria

Geetha Murugesan
CISA, CGEIT, CRISC, CDPSE, COBIT 5 Implementor and Assessor, CSA Start, ISO 22301:2019 LA, ISO 27001:2013 LA, ISO 31000:2018, ISO 9000:2015 LA
Principal Consultant, India

Martin Njogu Gichui
CISA, CISM, CGEIT, CRISC
ETHINK Global Solutions, Kenya

Maxwell Shanahan
CISA, CGEIT, FCPA, MACS, MIIA
Australia

Amit Sheth
CISA, CGEIT
SUN Pharmaceutical Industries Inc., USA

Caren Shiozaki
CGEIT, CDPSE, CEDS, LPEC
Fortium Partners, USA

Dirk Steuperaert
CISA, CISM, CRISC
Belgium

Patricia Voight
CISA, CISM, CGEIT, CRISC, CDPSE
Webster Bank, USA

Board of Directors

John De Santis, Chair
Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Niel Harper, Vice-Chair
CISA, CRISC, CDPSE, CISSP, NACD.DC
Chief Information Security Officer and Data Protection Officer, Doodle, Former Chief Information Security Officer, United Nations Office for Project Services (UNOPS), Germany

Stephen Gilfus
Managing Director, Oversight Ventures LLC, Chairman, Gilfus Education Group and Founder, Blackboard Inc., USA

Gabriela Hernandez-Cardoso
NACD.DC
Former President and CEO, GE Mexico, Independent Board Member, Mexico

Jason Lau
CISA, CISM, CGEIT, CRISC, CDPSE, CIPM, CIPP/E, CIPT, CISSP, FIP, HCISPP
Chief Information Security Officer, Crypto.com, Singapore

Massimo Migliuolo
Independent Board Member, Malaysia

Jamie Norton
CISA, CISM, CGEIT, CIPM, CISSP
Partner, McGrathNicol, Australia

Maureen O'Connell
NACD.DC
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

Erik Prusch
Chief Executive Officer, ISACA, USA

Asaf Weisberg
CISA, CISM, CGEIT, CRISC, CSX-P, CDPSE
Chief Executive Officer, introSight Ltd., Israel

Pamela Nigro
ISACA Board Chair 2022-2023 CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President, Security, Medecision, USA

Tracey Dedrick
ISACA Board Chair, 2020-2021
Former Executive Vice President and Head of Enterprise Risk Management, Santander Holdings, USA

Brennan P. Baybeck
ISACA Board Chair, 2019-2020 CISA, CISM, CRISC, CISSP
Senior Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

About ISACA

ISACA® (www.isaca.org) is a global community advancing individuals and organizations in their pursuit of digital trust. For more than 50 years, ISACA has equipped individuals and enterprises with the knowledge, credentials, education, training and community to progress their careers, transform their organizations, and build a more trusted and ethical digital world. ISACA is a global professional association and learning organization that leverages the expertise of its 180,000+ members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. It has a presence in 188 countries, including more than 225 chapter worldwide. Through the ISACA Foundation, ISACA supports IT education and career pathways for underresourced and underrepresented populations.

DISCLAIMER

ISACA has designed and created Artificial Intelligence Governance Brief (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Participate in the ISACA Online Forums:
engage.isaca.org/onlineforums

LinkedIn:
www.linkedin.com/company/isaca

X:
www.x.com/isacanews

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/

Artificial Intelligence Governance Brief