

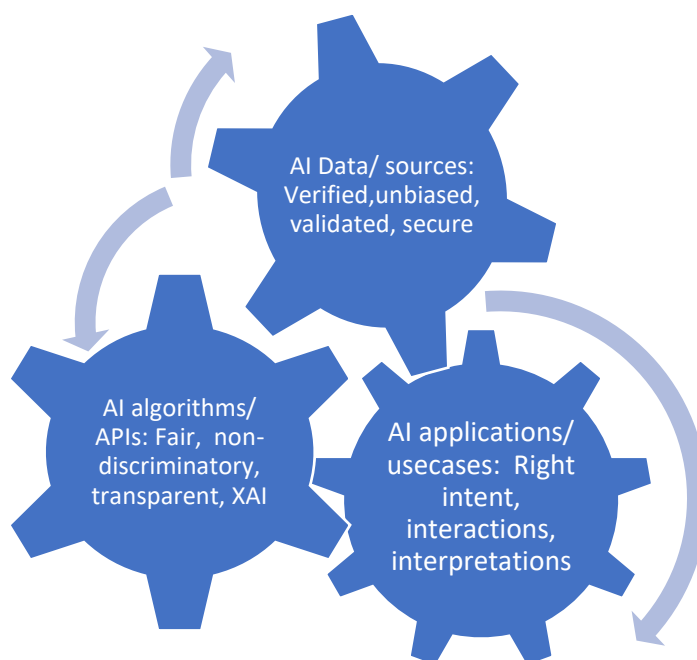
AISWITCH AI PRACTICE COOKBOOK: HOW TO ESTABLISH AI GOVERNANCE POLICIES WITH EVOLVING STANDARDS

Who should read this: Enterprise AI CoE leaders, CDO, CIO, CEO (for strategic AI initiatives), AI Business User Leaders, AI risk management professionals, data security & AI Solution Architects, AI Solutions & Service Providers

Why the need for standards and Regulations of Artificial Intelligence?

Given that AI applications are slated to proliferate in more than 80% Fortune 1000 organizations in next 3-5 years, global standards for the regulation of artificial intelligence are rapidly emerging and are more important now than ever before, for a variety of reasons:

- It is not enough to merely list out the cases of possible misuse of artificial intelligence. Identifying threats also mandates that we identify ways to minimize prevent and mitigate the impact of those threats. This is where the regulatory landscape of artificial intelligence becomes important.
- The technology of artificial intelligence is not only new, but it is a work in progress, ensuring that advancements occur every day. Fierce competition for the development and deployment of AI technologies is likely to emerge in the future, necessitating the use of legal standards to act as a deterrent to AI being employed for unethical purposes.



Vulnerable usecases of AI already range from misuse of personal data, to addictive AI i.e. targeted advertising with the aim of making users addicted to certain behaviors that can directly or indirectly generate revenues of businesses, without users' knowledge or consent.

What are the most prevalent existing and evolving standards?

Some of the existing & evolving standards governing artificial intelligence are:

- IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems-
- The IEEE Standards Association has the IEEE P7000 series of working groups, in AI standards, comprising of 14 groups, IEEE P7001, IEEE P7002, IEEE P7003, IEEE P7004, IEEE P7005, IEEE P7006, IEEE P7007, IEEE P7008, IEEE P7009, IEEE P7010, IEEE P7011, IEEE P7012, IEEE P7013, IEEE P7014 to address issues at the meeting point of technological and ethical concerns.
- European Union's General Data Protection Regulation (GDPR)

These ethical standards and regulations range over a number of ethical concerns and are used to monitor a number of potential risks across sectors

- With a mission to deploy technological advancements for the benefit of all humanity by aiming to educate, train and empower all stakeholders involved in the design and development of autonomous and involved artificial intelligence systems, the IEEE Global Initiative is broad system of standards to build a world powered by characterized by equal access to ethical technology.
- Regulating Organizations- IEEE Draft Model Process for Addressing Ethical Concerns during System Design (IEEE P7000) and Standard for Transparent Employer Data Governance (IEEE P7005) involve the ethical considerations and human rights issues to be factored in by organizations in concept exploration and development and transparency procedures to be followed by employers in collecting, storing and using employee data respectively.
- Rights of Minors- The Standard for Child and Student Data Governance (IEEE P7004) monitors the security of data collected from students and children in terms of regulating the organizations collected this data and the permitted use of this information
- Individual Privacy Rights- Standard for Personal Data Artificial Intelligence (AI) Agent (IEEE P7006) and Data Privacy Process(IEEE P7002) regulates the technical elements used to gain access to and use personal data of individuals and the privacy rules for the same.
- Use of Robotic Systems- The Ontological Standards for Ethically Driven Robots and Systems (IEEE P7007) and Standard for Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems (IEEE P7008) oversee the incorporation of

ethically driven methodologies into robotic systems and ethically driven nudging for robotic technologies.

- Put into effect in 2018, the GDPR levies strict penalties on those violating norms set for maintaining data privacy. Ranging from fairness, accuracy and transparency of the data collected, to limitations set on the amount, purpose and storage of personal data collected, the GDPR seeks to integrate confidentiality and accountability into the entire data collection process.

How to make these standards really work in an organization? How to put them in action?

Discussing globally evolving ethical standards must also involve exploring emerging artificial intelligence technologies being developed and deployed by global organizations. Regulation needs to take into account what exactly needs to be regulated, hence any discussion around ethical and legal standards of AI is incomplete without discussing globally evolving use-cases of AI.

The rapidly emerging use of AI by global organizations makes regulatory standards imperative for AI-powered businesses and operating models, since the scale of these technologies ensures that they have the greatest impact.

But, having the standards documented somewhere in the organization's repository of numerous policy documents, will clearly not work for AI usecases that are alive and kicking in a production environment. To bring them to everyday practice of AI in an enterprise:

- **Expand the scope of the standards beyond technology & data:** Policies are just as good as their executors. Current standards on GDPR and IEEE capture all the data and technology governance aspects reasonably well, with 3000+ articles and artefacts related to various generic to specific AI usecases. For example: general usage of transactional data to train AI fraud detection models, to specific policies related to decisions and actions taken by autonomous vehicles (e.g. the Perambulator problem).
While technology governance standards are important, they will work if and only if they are executed in conjunction with people, process and business governance systems and practices. The scope of technology standards must be broadened to include these aspects e.g. training, awareness building, risk measurement processes etc.
- **Build AI-powered autonomous systems to enforce and audit standards on the actual behavior, decisions and actions of autonomous systems on ground:** Humans monitoring and auditing of compliance and standards enforced in autonomous systems beat the entire purpose of having either the systems or the standards in the first place. This is because of the fact that the speed of these systems is their key virtue, that beats the latency of human decisions & actions. Only AI-based autonomous systems have the speed and accuracy of predictions

and actions with which they can monitor, prevent and/or control damages caused by autonomous AI applications' potential violation of any standards.

Action items next Monday Morning

Key actions	Key actors
Establish enterprise-level/ corporate-level AI governance policies across data, algorithms and applications, factoring in evolving standards like IEEE P7000 and GDPR.	AI CoE leaders, organizational AI governance councils/ steering committee
Mandate the AI solution architects and owners to train themselves on the AI governance policies and adhere to them in all their activities.	AI CoE leaders, solution architects, AI solution owners
Establish an internal audit team both for periodic as well as surprise/ anytime compliance checks and audits of all major/ critical AI-automation applications in the enterprise.	AI CoE leaders, solution architects, business leaders, AI solution owners
Share the AI governance audit reports with the executive leadership and risk management functions of the organization and seek their feedback to improve the systems and ensure adherence to the evolving standards.	AI CoE leaders, solution architects, business leaders, AI solution owners

...

For further information on techniques and systems: admin@aiswitch.org