REDCLOVER ADVISORS

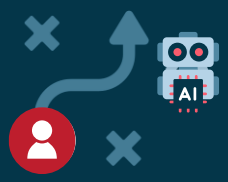
AI Governance Roadmap: Business Guide

www.redcloveradvisors.com | info@redcloveradvisors.com

REDCLOVER ADVISORS

AI GOVERNANCE

A Privacy-Centric Approach



Artificial intelligence (AI), and to a greater extent generative AI, are injecting new capabilities into how businesses operate — and these capabilities come with new risks and challenges.

As these tools mature and saturate the business ecosystem, laws and best practices are emerging for companies employing them. There isn't yet consensus on what AI policy should look like; however, by adopting the foundational principles of data privacy — the Fair Information Practices — you can position your AI program for success as frameworks evolve.

The Fair Information Practices

Transparency

Do you disclose to individuals how you process their information?

Accountability

Do you have an owner of your program and record-keeping on your practices?

Data Minimization

Do you only use the information necessary to achieve your business purposes?

Purpose Limitation

Do you only use information for the purpose it was collected and as noticed to the individual?

Individual Participation

Do you give people the ability to make choices about their information and exercise their rights?

Data Integrity

Do you have systems and processes to ensure information is accurate and up to date?

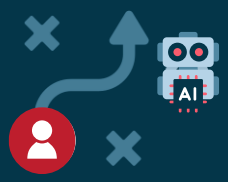
Security Measures

Do you protect information according to the level of risk it represents to the company and the individual?

REDCLOVER ADVISORS

AI GOVERNANCE

Identifying and Mitigating Privacy Risk



Identifying and mitigating risks that come from AI is essential to reaping the benefits in a responsible and ethical way. While there are certainly risks that live outside the realm of privacy, many AI risks do involve the processing of personal information. Companies can use strategies developed by and for data privacy to help identify the risks and develop appropriate measures to mitigate those risks.

AI ASSESSMENTS

Any time a company uses new technologies that interact with personal information, it should conduct a privacy impact assessment (PIA). Similarly, when a company implements AI technologies, it should conduct an AI assessment. Leverage your PIA template and process to kickstart your AI assessment process.

PRIVACY BY DESIGN & DEFAULT

The principles of privacy by design and default ensure companies build privacy protections into systems and processes from conception to sunset. When implementing AI tools and creating AI policies and processes, use these principles to guide your program.

PRIVACY ENHANCING TECHNOLOGIES

Data privacy programs encourage the use of de-identification technologies in any processing activity where personal information is not necessary to achieve the desired outputs. Assess your purposes for using AI and implement privacy enhancing technologies, like data masking, substitutional data, and encryption are used wherever possible.

AUDITING & TESTING

AI tools, systems, inputs and outputs should be reevaluated regularly to ensure they are working — and being used — as intended. Audit your systems to ensure de-identification is effective, eliminate biases, look for scope creepy and more. It's likely you already have a privacy and security review process for your information systems. Build your AI audits and testing to be compatible with your exiting audits and testing capabilities. And be sure to update your policies and processes as your organization's use of AI evolves.

www.redcloveradvisors.com | info@redcloveradvisors.com

Considerations When Using AI

Implementing AI tools should be done thoughtfully and with an eye on both the inputs and the outputs.

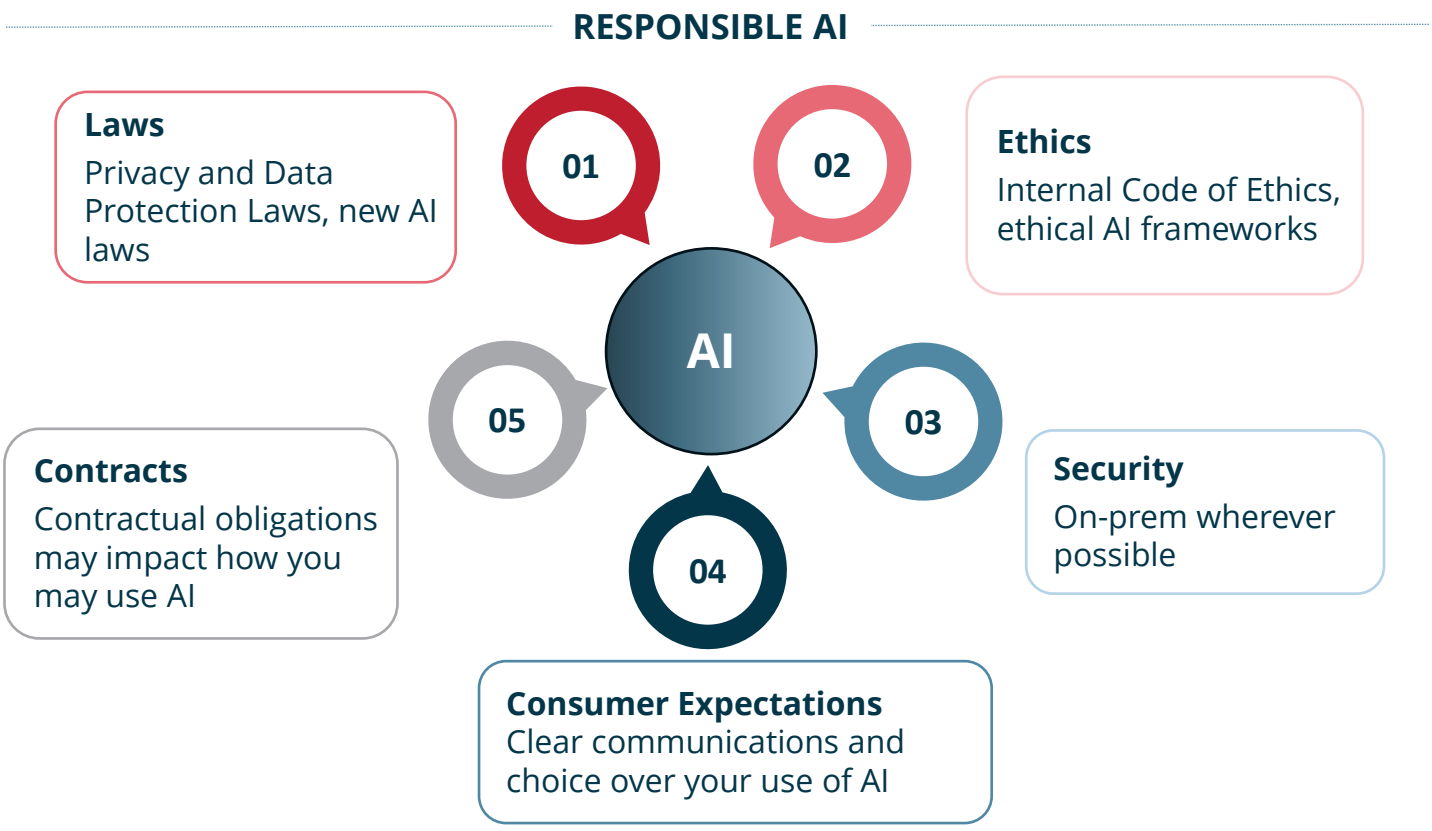
Laws: Ensure you know the privacy and data protection obligations and how they will apply to your use of AI.

Ethics: Your use of AI should follow your company's code of ethics and consider ethical AI frameworks like those published by NIST, the EU Parliament, and the EU Commission.

Contracts: Contracts may include rules and obligations about your processing of personal information, companies should ensure that any AI use of personal information obtained via contract complies with the contract.

Consumer expectations: Companies work hard to build trust in their customers, employees and others, make sure you consider their expectations and are clear in your notices, so you don't destroy that trust.

Security: Wherever possible, companies should implement AI tools on-prem to ensure personal information and other confidential company data isn't exposed to third parties.



Steps for Choosing AI Tools

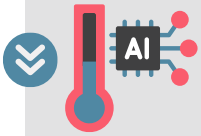
When choosing an AI tool to accelerate your business, be sure to start by understanding the purpose and goals you want the tool to achieve now and in the future. Then consider the following factors to ensure you get the right tool for your needs.

EFFECTIVENESS

Have clear goals for the tool and ensure it will work for your intended purposes.

COST & PRICING MODEL

Consider subscription fees, implementation and ongoing support to ensure the tool fits within your budget.

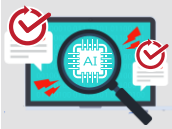


SCALABILITY

Brainstorm potential future uses and choose a tool that can scale to multiple and new uses.

RELIABILITY

Ensure the tool is regularly updated so models and data maintain their effectiveness.



COMPATIBILTY & EASE OF USE

Ensure the tool integrates with your existing systems and will cause minimal disruption to workflows.

SECURITY & COMPLIANCE

Wherever possible use on-prem as opposed to cloud tools. And either way be sure to review security and compliance protocols.

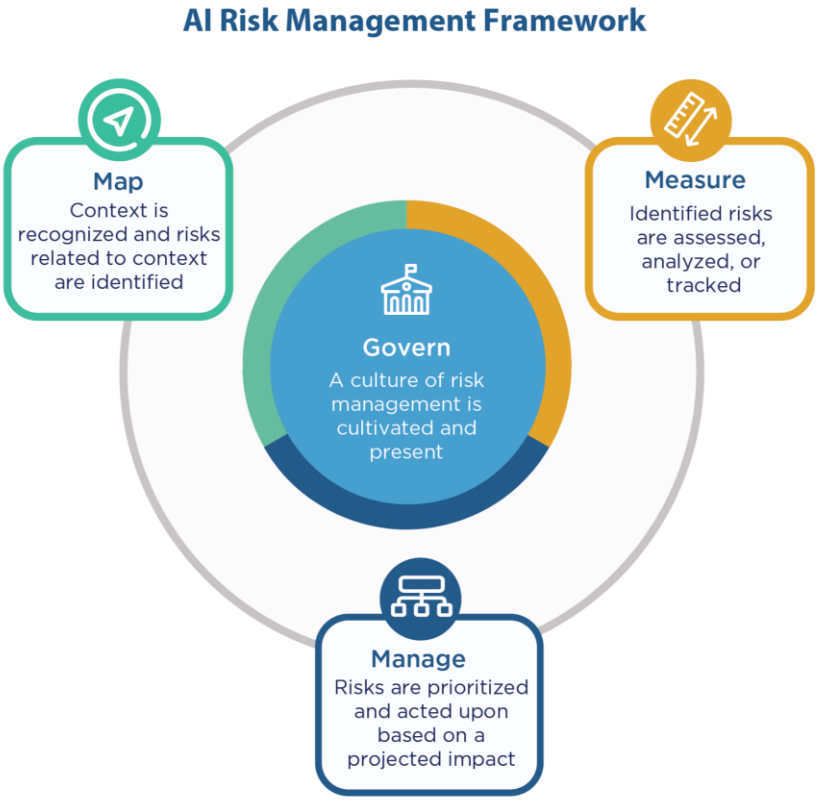
CUSTOMIZATION

Ensure you can customize the tool to meet your needs related to effectiveness and compliance.

SUPPORT

Make sure you can get the level of support you need within your budget.

The NIST AI Risk Management Framework



The National Institute of Standards and Technology has published a voluntary framework to help organizations design, develop, use and evaluate AI products, services and domains. At its core are the following functions:

Govern: Putting policies, processes and accountability mechanisms in place across the organization. Focus on diversity, equity, and inclusion throughout all phases and functions of the process.

Map: Understanding context and capabilities of the AI system. Getting full visibility of all parts of the process and the interdependencies. Understanding risk in each step of the process.

Measure: Identify appropriate metrics and apply across the organization. Ensure you measure for trustworthiness, security, privacy, fairness and bias, and that the levels meet your risk tolerance profile.

Manage: Monitor risk and prioritize risk mitigation in line with your organization's risk profile. Manage for maximum benefits and minimum negative impacts.

AI GOVERNANCE

Set Yourself Up for Success

AI GOVERNANCE COMMITTEE

The committee should include representatives from privacy, IT, security, legal, and marketing, compliance, HR and others as applicable. Responsibilities include strategic guidance and decision making around AI, increasing stakeholder engagement, and reviewing feedback from users and external partners.

AI INVENTORY

Inventory the AI tools currently in use by your organization and review the terms of service and privacy notice to understand how the tool uses your data and whether it is compliant with applicable laws, and/or used to train the AI model or system. Set up a regular cadence for updating the inventory.

MEASURE RISK

Conduct assessments to measure risk, such as AI assessments, privacy impact assessments, data protection impact assessments or transfer impact assessments where applicable.

REVIEW CONTRACTS

Prior to using personal information related to a contract in AI, ensure the contract allows the use of AI, identifies the purpose as within scope and has no other limitations on the processing activity.

POLICIES & PROCEDURES

Document policies and procedures specific to AI, and ensure you incorporate these new uses into existing policies. Ensure you cover applicable uses, procurement, risk assessments, system testing, metrics, training, and incident response. Regularly update this documentation to ensure compliance with emerging legislation.

AUDIT OUTPUT

Hallucinations and biases are common AI challenges. Make sure you have a process for human review of the AI outputs and processes to remedy any problems with the system.

TRAINING

Ensure employees know your policies around acceptable uses of AI tools. Incorporate AI into existing training programs and create specific AI training for employees who implement or regularly interact with these tools.