

AI governance checklist

*8 steps to establish AI
governance*

AI governance checklist

A guide to establishing AI governance.

Use this checklist as a framework to guide your organization through the process of establishing AI governance.

Action steps		Status
☐	1. Choose your AI governance team	
☐	Identify leaders within your organization to develop and champion AI governance. This typically includes your CFO, CIO and COO, although larger organizations might delegate some or most responsibilities to an AI governance body or working group.	
☐	Include a diverse set of role perspectives here. This is valuable because you want people who can help think about how to implement AI in different parts of your organization.	
☐	2. Level set for AI knowledge	
☐	Make sure everyone on your governance team understands AI, including the different types of AI like generative AI or agents, how the technology has evolved over the last few years and challenges or limitations like hallucinations.	
☐	Level set so that your whole governance team is working from the same common knowledge base.	
☐	3. Talk about AI dos and don'ts	
☐	Within your governance team, think about your AI dos and don'ts. What do you want to use AI for — and what do you not want it used for?	
☐	Consider do's like automating certain highly repeatable tasks or helping speed up the creation of sales proposals.	
☐	Establish don'ts like using AI to replace person-to-person relationships or writing completed blog posts for your website.	
☐	4. Decide which AI governance pillars fit your needs	
☐	Create a list of your AI governance pillars. When building this list, account for your dos and don'ts, the compliance requirements of your industry and other important factors like bias, security or sustainability.	

Action steps		Status
☐	4. Decide which AI governance pillars fit your needs (continued)	
☐	Pillar 1: Fairness and bias management. Depending on their training data, AI models can be at risk for showing bias towards certain groups based on characteristics like ethnicity or gender. Assess whether this could be a problem with AI tools you use, especially if those tools are trained on smaller datasets.	
☐	Pillar 2: Reliability and validity. The reliability of AI outputs depends heavily on the quality of the inputs. Consider whether you are feeding clean, organized data into your AI tools and regularly evaluate the outputs for accuracy.	
☐	Pillar 3: Privacy and security. Public AI models, especially, can represent major data privacy or security risks. Establish controls to make sure that sensitive or protected information doesn't end up getting shared with AI systems that shouldn't have access to it.	
☐	Pillar 4: Transparency and explainability. Do you understand how your AI models work and are being used within your organization? Transparency and explainability standards make sure these questions are regularly considered.	
☐	Pillar 5: Accountability and oversight. AI used without any human accountability or oversight can lead to serious risks in areas like bias, compliance and reputation. Set up guardrails to help ensure any AI use within your business is done in accordance with your governance framework and policies.	
☐	Pillar 6: Inclusiveness. In addition to avoiding bias, are your AI tools actively inclusive? Depending on the type of AI you are using, this may involve using models trained on diverse datasets that account for the wide range of the human experience, as well as making sure your tools are broadly accessible to users within your business.	
☐	Pillar 7: Legal and regulatory compliance. Legal and compliance requirements around AI use will only continue to grow, especially in regulated industries. Make sure your team knows the specific rules that affect AI use within your sector and takes ongoing action to help ensure you maintain (and can demonstrate) compliance.	
☐	Pillar 8: Vendor and third-party risk. If your business is using AI, your vendors and other third parties you may share information with almost certainly are as well. This can be a significant data privacy and security risk area, especially in regulated industries.	
☐	Pillar 9: Acceptable IP use. AI raises huge copyright and IP questions, many of which are unresolved. Be aware that AI usage that pulls from copyrighted or trademarked intellectual property could create liability for your business — even if done unintentionally.	
☐	Pillar 10: Sustainability. AI tools are powered by resource-hungry data centers. Think about your AI usage from a sustainability standpoint and consider taking actions like limiting AI for certain tasks or buying carbon offsets.	

Action steps		Status
☐	5. Collaborate with other stakeholders	
☐	Bring other AI stakeholders within your organization into the governance conversation. Seek out a wide, diverse range of perspectives here.	
☐	Establish open communication between your governance team and the rest of your organization.	
☐	6. Talk about any new governance processes you may need	
☐	Develop specific processes around areas like AI tool approval. You should know who signs off on implementing a new AI tool your team is interested in trying?	
☐	7. Clarify which AI tools are acceptable to use	
☐	Create share clear guidelines around which specific tools do you want your team to use and which you don't.	
☐	Clarify to your whole organization why certain tools are off limits. For example, a public, non-enterprise AI model will likely have unacceptable data privacy issues.	
☐	8. Write your formal AI policy	
☐	Pull together the work done by your governance team into a formal AI use policy. This can be as simple as downloading a sample policy and adjusting the details to fit the governance pillars and guidelines you've identified, but you can also write your own policy from scratch.	

Get help making AI work for you

Wipfli advises organizations on implementing AI, establishing governance, managing risks and delivering stronger operational outcomes. Let's talk about how we can help make AI work better for you.

[Contact us to learn more.](#)