

AI Compliance in 7 Steps

The constantly evolving regulatory landscape and volume of personal data for organizations mean that privacy and governance programs have to be dynamic. Maintain continuous compliance when you follow these seven steps.



REQUIREMENTS

RISK

COMPLIANCE

CERTIFICATION

1 Understand laws and requirements

2 Identify AI risk
3 Score and assess AI risk
4 Determine risk management activities

5 Track and measure compliance and risk
6 Report on risk and compliance

7 Demonstrate responsible AI practices

1 Understand what AI laws and compliance requirements apply to your business.

- What type of AI are you using (e.g., large language model (LLM), Foundation model)?
- How does your AI system process data, particularly if it uses personal information to train and/or make decisions?
- What are the potential impacts of the AI processing on individuals, like customers and employees?

2 Identify and understand risky activities in your business.

- Determine if your organization's processing would be considered "high-risk processing."
- Understand if any of your third-party vendors engage in "high-risk processing."
- Provide appropriate transparency and explainability.

3 Score and assess AI risk.

- Implement a system or methodology for classifying risks associated with AI use.
- Conduct the appropriate assessment required to identify potential risks to individuals and consequences for the organization
- Leverage your business's existing risk assessment procedures to incorporate AI or use external frameworks.

4 Determine risk management activities.

- Develop and document a plan for how your organization will mitigate AI risks.
- Prioritize risks based on their likelihood of occurring and the severity of the impact.
- Identify who's responsible for determining and implementing the controls to mitigate the risks.
- Enable a human to intervene in the AI processing at any time.

5 Track and measure AI risk and compliance.

- Keep up-to-date on existing and emerging privacy laws and AI compliance requirements.
- Sign up for compliance alerts and customizable reports to help stay on top of developments.
- Appoint dedicated individual(s) or team to communicate important updates and changes.

6 Continuously report on risk and compliance.

- Continually monitor the functionality and behavior of the AI system after it has been deployed.
- Regularly review the AI system's outputs to ensure it continues to function the way it's intended.
- Determine a set of activities if the AI system doesn't function properly.

7 Verify responsible AI practices with a third party.

- Engage a third party auditor or certification provider to verify you are doing things compliantly.
- Revisit or review your compliance regularly and especially when a new AI technology or related process is introduced.