

An aerial photograph of a river flowing through a lush green forest. The river is a light brown color, contrasting with the vibrant green of the surrounding trees. The image is used as a background for the left side of the page.

Guide to conducting AI impact assessments

NOVEMBER 2025

AI impact assessments are one of the most effective ways to turn responsible AI principles into practice, but they're still underused and often hard to operationalise.

Over the past few years, organisations have worked hard to define ethical AI principles and develop AI governance and usage policies—but progress often stalls when it comes to developing and conducting AI impact assessments. The result? A widening gap between rapid AI adoption and consistent risk oversight.

That gap isn't sustainable. With regulatory scrutiny increasing, public expectations shifting and productivity pressures mounting, organisations can't afford to delay AI deployment or ignore the risks.

Included in this guide

This guide provides a practical, repeatable approach to assessing and documenting AI risks and impacts. In it, you'll find:

- typical challenges and how to avoid turning assessments into paperwork exercises
- emerging practices that balance speed and rigour
- practical prompts, roles and checkpoints to integrate across the delivery lifecycle.

It's designed so you can move quickly, satisfy regulators and stakeholders, and keep trust at the core of every AI deployment.

What is an AI impact assessment?

Defining an AI impact assessment

AI impact assessments prompt organisations to critically assess and balance the risks and rewards relevant to AI systems or use cases. They also help identify and document the controls intended to mitigate identified risks.

The nomenclature around AI impact assessments is unsettled—they are also sometimes called AI risk assessments, AI impact and risk assessments, AI system impact assessments, or algorithmic impact assessments—often interchangeably.

AI impact assessments will increasingly play a role in helping organisations determine whether to include information about automated decision-making in their privacy policies, to comply with new APPs 1.7–1.9 and the Australian Government's Guidance for AI Adoption: Implementation practices.¹

AI impact assessments identify, assess, and respond to opportunities and potential risks and harms arising from AI use.²

Governance of AI Part 2: A director's guide to AI governance (AICD and HTI)

Why are AI impact assessments important?



Stay compliant: required in some cases, expected in many, they evidence how you identify and manage AI risks across the lifecycle and help meet obligations (eg compliance with new Australian Privacy Principles 1.7–1.9; CPS 230 Operational Risk Management).



Keep everyone aligned: they create a clear, shared picture of how each AI system works, what data it uses and how it will be applied so that teams aren't working from different assumptions.



Spot risks early: from bias and legal exposure to reputational or technical issues, assessments surface problems before they become costly or public.



Build trust: transparency isn't just a value, it's a proof point. Showing how you manage AI responsibly earns confidence from customers, employees and business partners.



Show accountability: documenting decisions and controls means you can demonstrate, at any time, that risks are being identified and managed—not left to chance.



Elevate more voices: good assessments bring in broad perspectives from those affected—employees, customers, communities—leading to fairer and more practical outcomes.

1 [Guidance for AI Adoption](#), Department of Industry Science and Resources

2 Other definitions are sometimes used for example
i. 'AI system impact assessment—a formal, documented process by which the impacts to individuals, groups of individuals and societies are considered by an organisation developing, providing, or using products or services utilising artificial intelligence.'
ISO/IEC 42005:2025 (Information Technology—Artificial Intelligence (AI))

ii. 'AI impact assessment tasks include assessing and evaluating requirements for AI system accountability, combating harmful bias, examining Impacts of AI systems, product safety, liability, and security, among others.'
NIST AI 100—1 Artificial Intelligence Risk Management Framework (AI RMF 1.0)—AI System Impact Assessment

Who, when and scope of an AI impact assessment

AI risks fundamentally change depending on the type and complexity of your AI systems. Risks often emerge from how the AI system behaves in different situations and use-cases, rather than only from software updates. They can rapidly amplify smaller issues into significant problems.

Section 3, [Guidance for AI Adoption](#), Department of Industry Science and Resources

Who should undertake an AI impact assessment?

- AI impact assessments should be undertaken by a cross-functional team with diverse skillsets, backgrounds, and experience.
- Ideally, the business owner looking to deploy the tool should not be the sole function undertaking the impact assessment.
- Allocation of responsibilities for conducting AI impact assessments should be documented and communicated.

Scope of AI impact assessments

AI impact assessments may be undertaken in respect of:

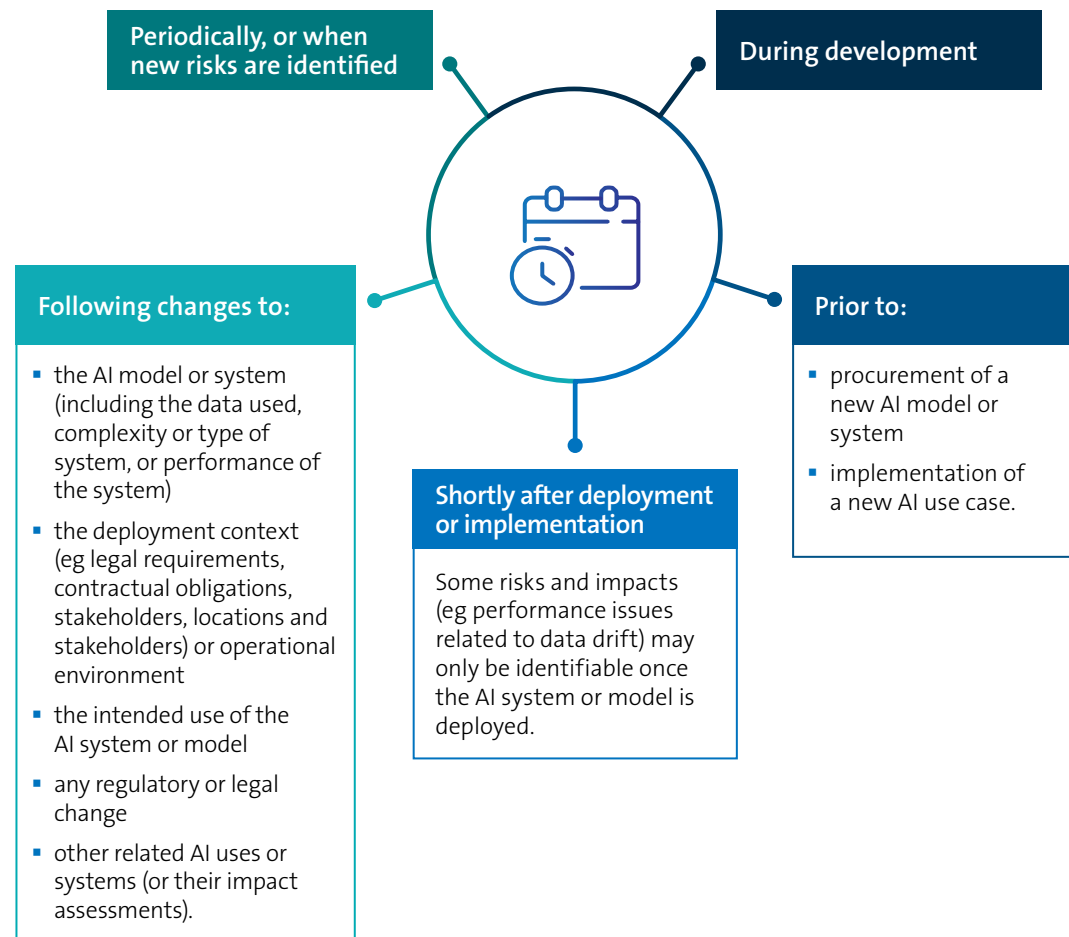
- an AI use case
- an entire AI system, or a component of the AI system (whether developed internally or by a third party).

Important considerations

As AI use proliferates, organisations are increasingly looking for ways to streamline their approach to assessing AI risks and impacts. One approach is to use a single AI impact assessment for multiple, comparable AI use cases. When doing this, it is important to:

- clearly define what is and isn't comparable
- record all AI use cases in the AI register³
- monitor the AI use cases to confirm whether they continue to meet the relevant profile and regularly review performance and impact against the initial assessment
- promptly initiate additional (or re-)assessments if material differences arise between profiles (having regard to data usage, functionality, risks etc).

When to conduct or re-perform an AI impact assessment



³ For more on AI systems registers, see [AI register template](#) | [Guidance for AI Adoption](#) | [Department of Industry Science and Resources](#).

How to conduct an AI impact assessment

For further guidance on conducting AI impact assessments, see [ISO/IEC 42005 Information technology—Artificial Intelligence \(AI\)—AI system impact assessment](#).

STEP 0 Precursor work

- Define your risk tolerance, identify risk categories (eg low, medium, high and unacceptable), and align these with your internal risk matrix.

STEP 1 Initiate an AI impact assessment

- Consider the triggers. Not every AI use case or feature roll out will require a detailed AI impact assessment.

STEP 2 Gather model, system and use case information

- Gather information on the AI system (including purpose, functionalities and capabilities), algorithm and model, deployment environment, data information and quality, and internal and external stakeholders.
- Identify, prioritise and review key stakeholders to understand their expectations, the impacts on those stakeholders, and to consider and elevate their voices as part of decision making around AI deployment.

Tip! Organisations often face challenges in obtaining information from third party AI model developers and system providers due to:⁴

- supply chain complexity and lack of upstream visibility
- reluctance to share proprietary or commercially sensitive information
- lack of engagement with those within the third parties that understand the AI model or system
- the 'black box' / explainability problem—ie third parties may not themselves understand the inner workings of the AI model or system.

STEP 3 Assess risks, harms and benefits

Identify:

- actual and potential benefits and harms (to individuals, groups of individuals, and organisations)

- legal, commercial and reputational risks such as failing to meet legal obligations, organisational commitments to ESG, diversity, inclusion and accessibility or programs supporting diversity, equity and fairness
 - risk mitigants,
- having regard to both *intended* uses, and reasonably foreseeable *unintended* uses, misuses and intentional abuses.

Tip! There should be alignment between this assessment and the AI principles defined in your AI Policy.

STEP 4 Identify, and test and monitor risk management strategies

Effective AI risk management also involves regularly checking how AI systems are working over the lifecycle, including creating and documenting criteria for reassessment over the lifecycle.

Tips!

- Consider expectations for reporting the results of the AI impact assessment and controls identified to address the impacts.
- Document approvals required as part of the AI system impact assessment process.

In 2024, MIT published its [AI Risk Repository](#), a dynamic catalogue of over 700 risks (today there are over 1600) cited in AI literature to date. The catalogue includes: (i) a causal taxonomy of AI risks that classifies how, when and why these risks occur; and (ii) a domain taxonomy of AI risks that classifies them into seven domains and 24 sub-domains.

Although not all of these risks will be relevant to all organisations or use cases, the catalogue is a helpful starting point in considering which risks should be contemplated in your AI impact assessment.



⁴ Daniel Berrick, [AI Governance Behind the Scenes, Emerging Practices for AI impact assessments](#), December 2024.

⁵ See section 3.2.3, [Guidance for AI Adoption](#), Department of Industry Science and Resources.

Five challenges and actions

Challenges

1. Adding AI-related processes to an already high volume and complexity of risk management processes can cause overwhelm which can in turn reduce their utility.

2. Third party providers are often unable or unwilling to provide relevant and sufficiently detailed information (eg, model developers and system vendors) to inform an AI impact assessment.

3. As AI systems and use cases proliferate, undertaking AI impact assessments becomes highly resource intensive. This can stall deployment.

4. There is the potential for frequent contextual and system changes (eg, legal and regulatory, different uses, technical changes) that can quickly alter the risk landscape, making it hard to anticipate risks.

5. The AI regulatory environment (globally and in Australia) is uncertain and evolving.

Actions

- Identify opportunities to streamline processes and reduce duplication.
- Clearly document (and educate staff on) the interaction between processes, documentation, artefacts and responsibilities.

- Identify the best contact to provide relevant and accurate information (it may not be the sales representative or the lawyer).
- Ask a small number of simple, direct questions.
- Interrogate the supplier's own AI governance posture and practices.

- Establish a triage system to determine which AI systems or use cases may pose an enhanced or unacceptable risk, aligned to the organisation's context and risk tolerance.⁶
- Identify opportunities to pre-approve AI use cases with similar profiles to reduce traffic in the system.

Document (and where possible automate) triggers to perform (and re-perform) AI impact assessments to ensure AI systems and use cases are regularly reviewed to identify changes to the nature or severity of relevant risks.

Continue to develop, document and implement sound AI governance policies and processes.

⁶ See section 3, [Guidance for AI Adoption](#), Department of Industry Science and Resources.

Key contacts



Valeska Bloch

Partner, Head of Cyber
T +61 2 9230 4030
Valeska.Bloch@allens.com.au



Isabelle Guyot

Partner
T +61 2 9230 4752
Isabelle.Guyot@allens.com.au



Gavin Smith

Partner, Practice Leader —
Technology, Media and
Telecommunications
T +61 2 9230 4891
Gavin.Smith@allens.com.au



Phil O'Sullivan

Partner, Health Sector Leader
T +61 2 9230 4393
Phil.O'Sullivan@allens.com.au



Jessica Mottau

Partner
T +61 2 9230 4587
Jessica.Mottau@allens.com.au



Emily Turnbull

Partner
T +61 3 9613 8711
Emily.Turnbull@allens.com.au



David Rountree

Partner
T +61 7 3334 3368
David.Rountree@allens.com.au



Elyse Adams

Partner
T +61 3 9613 8534
Elyse.Adams@allens.com.au



Dominic Anderson

Partner
T +612 9230 4099
Dominic.Anderson@allens.com.au



Lisa Kozaris

Chief Innovation
and Legal Solutions Officer
T +61 3 9613 8944
Lisa.Kozaris@allens.com.au

[Our latest thinking on AI](#)