aptem.
Intelligent technology®

AI Suitability and Impact Assessment

Starter template

A template for your organisation to assess the impact of a specific AI tool, model, or use case before procurement or deployment.

Provided by Aptem

Version: 1.0

Owner: [AISIA Owner]

Status: [Draft / Active]

Date: [Day Month Year]

Audience: customer-facing starter template

aptem.
Intelligent technology®

Contents

Follow us on LinkedIn and YouTube

www.aptem.co.uk

29 May 2026

aptem.
Intelligent technology®

How to use this template

An AI Suitability and Impact Assessment (AISIA) is the primary way your organisation documents how it has evaluated the effects of an AI-supported service on its users, its staff, and on the organisation itself. It identifies inherent risks, the potential impact on stakeholders, and the controls in place to prevent or mitigate them.

An AISIA complements, rather than replaces, a Data Protection Impact Assessment (DPIA). A DPIA covers the personal-data risks under UK GDPR. An AISIA covers the broader ethical, operational, and user-centred implications of using AI.

When to complete an AISIA

Complete an AISIA whenever your organisation:

- Implements a new system, tool, or technology that uses AI.
- Introduces a new use case for a previously approved AI-supported tool.
- Adds AI functionality to an existing system, tool, or service.

How to complete an AISIA

1. Identify each distinct use case for the AI. Each use case has its own impact, so each one needs its own AISIA.
2. Copy this template, name it after the supplier or tool and the use case (for example, "AISIA - [Supplier] - [Use case]"), then fill it in.
3. Replace every placeholder in square brackets with your own content. Delete the guidance text in italics once the answer is in place.
4. Pair the AISIA with a DPIA where personal data is involved. The two run alongside each other.
5. Route for sign-off (see Section 5).

AI risk classification

Use the same three-tier model as your AI use and governance charter:

- AI-Low. Little or no effect on individuals or consequential decisions.

aptem.
Intelligent technology®

- AI-High. Influences outcomes for individuals or processes personal data with potential impact on rights or eligibility.
- AI-Prohibited. Use of AI that breaches law, regulation, or the charter. Stop here if the assessment lands in this tier.

Follow us on LinkedIn and YouTube

www.aptem.co.uk

29 May 2026

aptem.
Intelligent technology®

1. Overview

Record the essentials at a glance. This block is the first thing a reviewer sees.

Field	Value
Supplier or tool	[Supplier name] - [tool URL]
Use case	[Brief one-line description of the use case]
Assessment date	[DD Month YYYY]
Last reviewed date	[DD Month YYYY]
Assessed by	[Name, role]
AI risk tier	[AI-Low / AI-High / AI-Prohibited]
AI incident log	[Link to incident log, or "None to date"]
Related DPIA	[Link to DPIA, or "Not required" with rationale]

aptem.
Intelligent technology®

2. Implementation risks

Complete one AISIA per use case, as the impact varies by how the AI is used. Replace italicised guidance with your own answer.

Category	Question and guidance	Your answer
Use case	**Describe the use case.** How does your organisation or its users interact with the AI functionality being assessed? How is the AI functionality integrated, and with which existing systems? Which users (staff, service users, external) are affected?	[Your answer]
Data	**What data does the AI have access to?** Is any personal, learner, employee, customer, or other sensitive data processed by the AI system? Consider both the overall tool and the AI-specific functionality.	[Your answer]
Privacy risks	**What AI technologies are used, and for what purpose?** Examples: large language model for drafting, machine learning for prediction, computer vision for document scanning.	[Your answer]
	How could the AI reveal personal data unintentionally? Consider what other systems and data the AI has access to, directly or indirectly.	[Your answer]
	How is the principle of 'data protection by design' applied? Only applies if personal data is being handled.	[Your answer]

	Is user data or organisational IP being used to train the underlying AI model? Yes or No. If No, explain how this is achieved (for example, enterprise contract, zero data retention, opt-out).	[Your answer]
User impact and experience	**Is the user informed that AI is being used?** Yes or No. If Yes, describe how (in-product disclosure, terms of service, user training).	[Your answer]
	Is there a human in the loop before any decision is made or content is presented? Describe the human review point.	[Your answer]
	Are users able to opt out of the AI functionality, or request a human alternative? Yes or No. If Yes, describe the route.	[Your answer]
	How is bias minimised or adjusted for? How are bias, explainability, and transparency managed? Reference any supplier documentation or model card.	[Your answer]
	Have diverse datasets been used in development and testing? Reference any supplier documentation on training data composition.	[Your answer]
Operational risks	**How is the risk of harmful, incorrect, or misleading content avoided or minimised?** Examples: human review, content filters, user training, monitoring of outputs.	[Your answer]

	Is there a risk of intellectual property or copyright infringement from public use of AI-generated output? How is this managed?	[Your answer]
	Fallback procedures. Describe what happens if the AI fails or produces unsafe responses. What is the manual or alternative process?	[Your answer]

aptem.
Intelligent technology®

3. Third-party AI system risks

Complete the table below for the AI system itself. The supplier or their public documentation will usually answer most of these. Link to supplier documentation where available.

Question and guidance	Your answer
Confirm the use case. A one-line summary of how this AI system is being used by your organisation. Should match Section 2.	[Your answer]
Has the underlying AI signed up to the EU AI Act, or made a public commitment to align with it? Reference public documentation.	[Your answer]
Does the supplier comply with ISO/IEC 42001 or other AI governance frameworks? If yes, list certifications and standards (for example, ISO 27001, SOC 2, ISO 42001).	[Your answer]
How could the AI reveal personal data unintentionally? From the supplier's perspective, given the data they hold.	[Your answer]
Is information sent to the AI being used to train the underlying model? Yes or No. Reference the supplier's documented position. Note any plan-specific or enterprise-only opt-outs.	[Your answer]
How does the AI system minimise or adjust for biased outcomes? Reference system cards, model cards, or research publications.	[Your answer]
Have diverse datasets been used in development and testing? Reference system cards or training-data documentation.	[Your answer]

How does the AI system avoid or minimise the risk of generating harmful, incorrect, or misleading content? Safety mitigations, red-teaming, content filters.	[Your answer]
What are the data leakage or model inversion risks? Reference supplier documentation. If unknown, note this and flag for review.	[Your answer]
How is data protected during processing? Encryption in transit and at rest, data residency, sub-processors.	[Your answer]

aptem.
Intelligent technology®

4. Additional comments

Use this section to capture anything that does not fit elsewhere. Examples include pending integrations that will need re-assessment, known caveats, time-bound restrictions, or supplier change-control notes.

Topic	Comments
[Topic, for example, pending integration]	[Your comment]
[Topic]	[Your comment]

aptem.
Intelligent technology®

5. Sign-off

An AISIA must be signed off before the AI tool, model, or use case is put into operation. The sign-off chain confirms that the implementation, third-party, and operational risks have been assessed and accepted.

This AISIA must be signed off by at least one of:

- A head of department or service area.
- A member of [Organisation]'s executive or senior leadership team.
- The Compliance lead, Data Protection Officer, or AI Charter Owner.

High-risk cases (AI-High) require sign-off from [senior leadership / board] in addition to the above.

Sign-off record

Role	Name	Date	Signature
[Role, e.g. Head of Department]	[Name]	[DD Month YYYY]	
[Role, e.g. Compliance lead]	[Name]	[DD Month YYYY]	
[Role, e.g. Executive sponsor]	[Name]	[DD Month YYYY]	