INTAI

DOWNLOADABLE CHECKLIST

RISK & ASSURANCE

AI Assurance Checklist

Check whether an AI system has sufficient evidence, testing, documentation, controls and ongoing monitoring to support confidence in its operation.

INTAI LIMITED
AI Governance & Assurance Consultancy

www.intai.co.uk
2026 Edition

AI Assurance Checklist

This checklist helps you assess whether you have genuine evidence — not just confidence — that a given AI system is operating as intended, and whether that evidence would hold up to scrutiny from a regulator, auditor or customer.

1 Documentation & Evidence

- ☐ **Is there documentation describing what the AI system does and how it is intended to be used?**
  Without this, it is difficult for anyone other than the original builder to assess or govern the system.
- ☐ **Is there a record of the data used to build, train or fine-tune the system?**
  This is foundational evidence for assessing bias, fairness and regulatory compliance.
- ☐ **Is there documentation of the system's known limitations and appropriate use boundaries?**
  Systems used outside their intended boundaries are a common, avoidable source of poor outcomes.

2 Testing & Validation

- ☐ **Has the system been tested for accuracy and reliability against a representative set of real-world scenarios?**
  Testing only against convenient or idealised cases provides limited real assurance.
- ☐ **Has the system been tested specifically for fairness across relevant groups?**
  This should be a deliberate test, not an assumption based on overall accuracy figures.
- ☐ **Has the system been tested for how it handles edge cases and unusual inputs?**
  Edge case behaviour is often where the most consequential failures occur.
- ☐ **Has testing been repeated after any material change to the system or its data?**
  Assurance evidence gathered before a material change does not necessarily hold true afterwards.

3 Monitoring

- ☐ **Is the system's performance actively monitored once it is live, not only tested before deployment?**
  Performance can degrade over time as real-world data and conditions shift away from the original training context.
- ☐ **Are there defined thresholds that trigger a review if performance changes materially?**
  Monitoring without defined thresholds tends to generate data that nobody consistently acts on.

- [ ] **Is monitoring data reviewed by someone with the authority to act on it?**
  Monitoring that produces reports nobody reviews provides limited practical assurance.

4 Independent Review

- [ ] **Has the system been reviewed by someone independent of the team that built or deployed it?**
  Independent review catches issues that those close to a system are more likely to overlook.

- [ ] **For higher-risk systems, has external or third-party assurance been considered?**
  This is not necessary for every system, but is increasingly expected for higher-risk or public-facing use cases.

5 Incident & Issue Management

- [ ] **Is there a process for logging and investigating issues identified with the system's outputs?**
  Without a formal process, issues are more likely to be handled inconsistently or not tracked at all.

- [ ] **Are lessons from identified issues fed back into how the system is monitored or improved?**
  Assurance activity that does not lead to improvement provides only partial value.

6 Continuous Assurance

- [ ] **Is assurance treated as an ongoing activity, rather than a one-time exercise completed before launch?**
  AI systems, and the environments they operate in, both change over time in ways that can affect their reliability.

- [ ] **Is there a scheduled cadence for reassessing assurance evidence for each system?**
  This should scale with the system's risk tier — higher-risk systems warrant more frequent reassessment.

- [ ] **Would the organisation be able to produce this assurance evidence credibly if asked by a regulator, auditor or customer?**
  This is a useful practical test of whether assurance activity is genuinely embedded, or exists only informally.

HOW TO SCORE THIS CHECKLIST

This checklist works best applied per system, particularly for anything tiered Limited risk or above in your governance framework. A system with multiple 'No' answers should not be assumed safe to continue operating without further assurance work.

INTAI

Need help acting on this checklist?

INTAI works with SMEs, public sector bodies and larger organisations across Europe to turn checklist findings into a practical, proportionate AI governance programme — from strategy and policy through to risk management and regulatory readiness. If you would like support closing the gaps this checklist has identified, our team is glad to help.

www.intai.co.uk | hello@intai.co.uk

© 2026 INTAI Limited. This checklist is provided for general guidance purposes only and does not constitute legal, regulatory or professional advice. Organisations should adapt it to their own context and seek independent advice where appropriate.