INTAI

DOWNLOADABLE CHECKLIST

RISK & ASSURANCE

AI Risk Checklist

Identify common AI risk areas across data, privacy, security, bias, reliability, operations, regulation and organisational reputation.

INTAI LIMITED
AI Governance & Assurance Consultancy

www.intai.co.uk
2026 Edition

AI Risk Checklist

This checklist gives SMEs and public sector organisations a structured way to scan for the risk areas most commonly associated with AI systems, before those risks materialise into an incident, a regulatory finding, or reputational harm.

1 Data & Privacy Risk

- ☐ **Has the lawful basis for processing personal data through this AI system been established?**
  This applies under GDPR whenever personal data is involved, including data used to train or fine-tune a model.
- ☐ **Has data minimisation been considered — is only necessary data being used?**
  AI systems can create pressure to collect or retain more data than is actually required for the task.
- ☐ **Is there clarity on where data processed by the AI system is stored and by whom?**
  This includes understanding whether data leaves the EU/EEA and what safeguards apply if it does.
- ☐ **Has a Data Protection Impact Assessment been considered or completed, where required?**
  This is typically required where processing is likely to result in high risk to individuals' rights.

2 Security Risk

- ☐ **Has the AI system been assessed for standard cybersecurity risks, not only AI-specific ones?**
  AI tools are still software, and inherit the same access control, patching and configuration risks as any other system.
- ☐ **Has the risk of prompt injection or manipulation been considered for generative AI systems?**
  This is an AI-specific risk category that traditional security assessments may not automatically cover.
- ☐ **Is access to the AI system and its outputs appropriately restricted and logged?**
  Uncontrolled access increases both the risk of misuse and the difficulty of investigating an incident.
- ☐ **Has the security posture of any third-party AI vendor been assessed, not assumed?**
  Vendor security failures become the organisation's risk the moment the vendor is handling organisational or customer data.

3 Bias & Fairness Risk

- ☐ **Has the AI system been tested for differential performance or outcomes across different groups?**
  Bias can emerge even without intent, particularly where training data underrepresents certain groups.

- ☐ **Is there a way to detect if the system's outputs become less fair or accurate over time?**
  Models and the data they operate on can drift after deployment in ways that were not present during initial testing.

- ☐ **Has the system been assessed for risk of unfair outcomes specific to its use case?**
  The nature of fairness risk varies significantly between, for example, a recruitment tool and a demand-forecasting tool.

4 Reliability & Safety Risk

- ☐ **Has the system been tested for how it behaves with unusual, incomplete or adversarial inputs?**
  Real-world use rarely matches the clean conditions of initial testing.

- ☐ **Is there a clear understanding of the consequences if the system produces an incorrect or unreliable output?**
  This should be assessed specifically, not assumed to be low-impact by default.

- ☐ **Is there human oversight appropriate to the potential consequences of an incorrect output?**
  Higher-consequence use cases warrant a correspondingly higher level of human review before action is taken.

5 Operational Risk

- ☐ **Is the organisation dependent on a single AI vendor with no reasonable fallback if service is disrupted?**
  Concentration risk is easy to overlook when a tool has become embedded in day-to-day operations.

- ☐ **Has the impact of the AI system being unavailable been assessed?**
  This is particularly important where a process has come to rely on the AI system with no manual fallback in practice.

- ☐ **Are staff able to recognise when an AI system is behaving unexpectedly?**
  Without this awareness, unusual outputs may be accepted and acted upon without question.

6 Regulatory & Legal Risk

- ☐ **Has the AI system been assessed against relevant EU AI Act risk categories?**
  This determines the specific obligations that apply, which vary significantly by risk tier and by your role as provider or deployer.

- ☐ **Has the system been assessed for compliance with sector-specific regulation, where applicable?**
  Financial services, healthcare, education and public sector bodies often face additional regulatory requirements.

- ☐ **Is there a process for monitoring regulatory change relevant to this system?**
  AI regulation across Europe is still developing; a system compliant today may face new obligations within the next year or two.

7 Reputational Risk

- ☐ **Has the organisation considered how this AI system's failure or misuse would be perceived externally?**
  Reputational exposure can exceed direct financial or operational impact, particularly for public-facing use cases.

- ☐ **Is there a plan for communicating transparently if something goes wrong with this system?**
  A credible response plan prepared in advance is far more effective than one improvised during an active incident.

HOW TO SCORE THIS CHECKLIST

Treat any 'No' answer in Data & Privacy Risk or Regulatory & Legal Risk as a priority — these carry the most direct compliance exposure. Use the remaining sections to build a fuller picture of operational and reputational exposure once the compliance-critical gaps are addressed.

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.