



# AI without rules is a risk

How to ensure transparency, accountability, and safe AI use in your organization

---

A whitepaper by Laurens Vandebergh, newTera  
Business Development Manager AI and Project Manager  
2026

# Executive Summary

AI offers enormous opportunities, but also comes with responsibilities. Organizations that deploy AI without thinking about ethics, safety, and transparency run risks that are difficult to repair after the fact: reputational damage, data breaches, legal liability, or simply a loss of trust.

This whitepaper is about Diligence: the fourth and perhaps most underestimated core competency within AI Fluency. Diligence addresses the question: how do you ensure that AI use in your organization is not only effective, but also responsible, transparent, and demonstrably safe?

The central message: responsible AI use is not a brake on innovation. It is the foundation on which sustainable AI adoption is built. Organizations that take Diligence seriously build trust with employees, clients, and partners, and are better positioned as regulations tighten.

*Think of AI the way you think about driving: your focus is not just on getting from A to B as fast as possible. You also follow the rules of the road and watch out for other people. AI use works exactly the same way.*

## The problem: AI use without guardrails

Most organizations that start working with AI focus on what AI can do. Less attention goes to the question of how AI should be deployed responsibly. That is understandable: the technology moves fast and the pressure to keep up is real. But the absence of guardrails creates creeping risks.

The European AI Regulation (EU AI Act), which is being phased in from 2025 onwards, makes clear that responsible AI use is no longer a matter of choice. Organizations that invest now in governance and transparency will not be scrambling to catch up later.

### Three signs that Diligence is missing

Do you recognize any of these in your organization?

- Employees use random AI tools without knowing what data those tools process or where that data goes.
- There is no policy on when to disclose that AI played a role in a document, report, or piece of advice.
- No one knows exactly who is responsible if AI-supported work contains errors or causes damage.

These are not hypothetical scenarios. They play out daily in organizations that enthusiastically embrace AI without a foundation of clear rules. The solution does not start with a thick policy document, but with awareness and a few clear agreements.

## What is Diligence within AI Fluency?

Diligence is the fourth core competency within the 4D framework of AI Fluency. While the other three competencies, Delegation, Description, and Discernment, are primarily about working with AI effectively and efficiently, Diligence is about the ethical and safe side of that collaboration.

Diligence works at three levels:

| CREATION DILIGENCE            | TRANSPARENCY DILIGENCE             | DEPLOYMENT DILIGENCE          |
|-------------------------------|------------------------------------|-------------------------------|
| Consciously choosing which AI | Being open about the role of AI in | Taking responsibility for AI- |

| <i>system to use and how</i>                     | <i>your work</i>                           | <i>supported output</i>                        |
|--------------------------------------------------|--------------------------------------------|------------------------------------------------|
| What data am I sharing? Is this system approved? | Does my client know that AI produced this? | Have I verified the facts before sending this? |

## Creation Diligence: choosing consciously

Before using AI, ask yourself a number of critical questions. Which system am I using, and who manages it? What data am I sharing, and who has access to it? Does this use align with my organization's policies and my own values?

This is not a bureaucratic exercise. It is the professional responsibility that comes with any use of AI, just as you think about who you copy on an email before hitting send.

## Transparency Diligence: being open about AI

People have the right to know when AI has played a significant role in content or decisions that affect them. Transparency Diligence is about the question: when do you disclose that, to whom, and how?

Expectations around transparency differ by context. An academic paper holds different norms than an internal memo. But the basic rule is simple: be honest about the role of AI when that role matters to the recipient.

## Deployment Diligence: taking responsibility

AI can make mistakes. Hallucinations, biases in output, misinterpretations. Anyone who shares AI-supported work with the outside world is responsible for its quality and accuracy. Not the AI, but you.

Deployment Diligence means: verify facts, check for bias, and make sure the output is correct before you distribute it. It is the final line of defense before AI-supported work leaves the organization.

## Concrete risks and how to mitigate them

The overview below lists the most common risks of careless AI use, what can concretely go wrong, and how to reduce the risk.

| RISK                          | WHAT CAN GO WRONG                                                  | HOW TO MITIGATE IT                                                             |
|-------------------------------|--------------------------------------------------------------------|--------------------------------------------------------------------------------|
| <b>Data leakage</b>           | Confidential information ends up with an external AI provider      | Only use approved systems; never share personal data or business secrets       |
| <b>Hallucinations</b>         | AI presents incorrect facts with great confidence                  | Always verify factual claims, especially in external communications            |
| <b>Bias in output</b>         | AI reproduces biases from training data, e.g. in recruitment       | Actively assess AI output for fairness; use it as a tool, not a final judgment |
| <b>Unclear accountability</b> | No one feels ownership of AI-supported work                        | Make explicit who is responsible for the end result                            |
| <b>Reputational damage</b>    | Incorrect or inappropriate AI output reaches clients or the public | Introduce a review step for AI-supported external communications               |

None of these risks is inevitable. All of them are manageable with awareness, clear agreements, and a culture in which employees feel safe to ask questions about AI use.

# What does Diligence require from an organization?

Diligence is not a task for the IT department or the compliance officer alone. It is a shared responsibility that needs to be embedded in policy, culture, and daily working practices.

## Policy: clear frameworks for everyone

An AI policy does not need to be exhaustive to be effective. A concise document answering the five most pressing questions already gives employees a solid foundation. Which tools are approved? What data may you share? Who is responsible for what?

| GOVERNANCE QUESTION                                 | KEY CONSIDERATION                                                         |
|-----------------------------------------------------|---------------------------------------------------------------------------|
| Which AI tools are approved for use?                | Maintain an approved list; don't ban everything, but give clear direction |
| Which data may be shared with AI?                   | Explicitly distinguish between internal, confidential, and personal data  |
| Who is responsible for AI output?                   | Assign an owner per type of AI task or department                         |
| How transparent are we toward clients and partners? | Determine when you disclose that AI has played a role                     |
| How do we keep employees up to date on the rules?   | Regulations and best practices change quickly; schedule periodic updates  |

## Culture: safety to ask questions

The best policy fails if employees are afraid to admit that they have doubts about responsible AI use. Organizations that create a culture in which asking questions is normal and mistakes are discussable learn faster and prevent bigger problems.

## Awareness: structural, not one-off

AI and the regulations around it evolve rapidly. A one-time training is not enough. Organizations that take Diligence seriously ensure periodic updates, actively share relevant developments, and make responsible AI use part of existing quality and compliance processes.

## The EU AI Act: what you need to know

The European AI Regulation (EU AI Act) categorizes AI applications by risk level. High-risk applications, such as AI in recruitment, credit scoring, or medical diagnosis, are subject to strict requirements around transparency, oversight, and documentation. Transparency obligations also apply to lower-risk applications. Organizations that establish a governance foundation now will be better prepared for the obligations coming into force in the years ahead.

## How to get started: from awareness to policy

Diligence does not need to start with a large-scale initiative. A phased approach is more effective and more achievable:

- **Step 1** — Raise awareness: discuss with your team which AI tools are currently in use and what questions that raises about data, responsibility, and transparency. You do not need to have all the answers yet.
- **Step 2** — Set guardrails: formulate five basic agreements about AI use in your organization. Which tools are acceptable? What should you never share? Who is responsible for what? Starting small works better than waiting for the perfect policy.

- **Step 3** — Embed it: make Diligence part of existing processes. Add an AI review step to external communications. Include AI use in performance conversations. Keep your policy current.

An AI Readiness Assessment maps out how your organization currently scores on Diligence and the other AI Fluency competencies, where the biggest risks lie, and which steps will have the most impact.

## Conclusion

Deploying AI without rules is not bold, it is reckless. The risks are real, but they are manageable. Organizations that take Diligence seriously are not just building safe AI use, they are building trust. With employees who know what is and is not allowed. With clients who can rely on AI being used responsibly. With partners who can see that your organization thinks ahead.

Responsible AI use is not a brake on innovation. It is the foundation on which sustainable innovation is built.

### Want to know how your organization scores on AI Diligence?

newITera's AI Readiness Assessment maps out where your people, processes, and governance stand today, and what the next concrete step is.

Contact us at [laurens.vandebergh@newitera.nl](mailto:laurens.vandebergh@newitera.nl) or visit [www.newitera.nl](http://www.newitera.nl)

## About newITera & Laurens Vandebergh

newITera is a Dutch IT consultancy based in Beuningen, Gelderland. Founded in 2011, initially as a specialized SAP firm, newITera has grown into a broad digital transformation partner. Today, newITera combines deep SAP expertise with services in data analytics, AI, cloud strategy, and low-code platforms. With a team of more than a hundred consultants, newITera serves leading enterprises and multinationals across their full digital transformation journey. What sets newITera apart is its combination of early adoption and deep specialization, as an independent partner that values human connection just as highly as technical excellence.

Laurens Vandebergh is Business Development Manager AI and Project Manager at newITera. With a broad background in technology and organizational change, he guides organizations in defining their AI strategy, conducting an AI Readiness Assessment, and realizing concrete use cases.

Contact: [laurens.vandebergh@newitera.nl](mailto:laurens.vandebergh@newitera.nl) | [www.newitera.nl](http://www.newitera.nl)