AI Readiness Checklist for Leaders

12 questions to check if your organisation is ready for AI-powered fraud, Shadow AI and decision-making under pressure.

AI readiness is not only about adopting new tools. It is about making sure your people know how to use AI safely, verify critical requests and respond when something feels wrong.

Use this checklist to assess whether your organisation is prepared for AI-powered threats, Shadow AI and decision-making under pressure. Mark one answer for each question: **YES / NO / NOT SURE**

Core Idea

AI does not hack systems first.
It hacks decisions.

RECOGNISE. VERIFY. RESPOND.

SECTION 1

AI Usage Visibility

Understand how AI is already being used internally, and where the hidden gaps are.

Question	YES	NO	NOT SURE
1. Do you know which AI tools your employees are already using at work?	☐	☐	☐
2. Do you have clear rules on what data must never be uploaded to public AI tools?	☐	☐	☐
3. Do employees know when AI-generated content requires human review before it is used?	☐	☐	☐

SECTION 2

Decision Verification

Make sure people verify AI-generated output before it influences important decisions.

Question	YES	NO	NOT SURE
4. Can a payment, contract, access request or data transfer be approved by voice, email or video alone?	☐	☐	☐
5. Do you have a multi-channel verification protocol for urgent, unusual or high-risk requests?	☐	☐	☐
6. Do managers know how to verify a request that appears to come from the CEO, CFO or another trusted person?	☐	☐	☐

SECTION 3

AI-Powered Attacks

Voice cloning, deepfake video and AI-generated phishing are active tools used by sophisticated threat actors targeting business leaders.

Question	YES	NO	NOT SURE
7. Have your leaders been briefed on voice cloning, deepfake video meetings and AI-generated phishing?	☐	☐	☐
8. Do employees know how to recognise manipulation based on urgency, authority, fear or secrecy?	☐	☐	☐
9. Do you have a clear escalation path when someone suspects an AI-powered fraud attempt?	☐	☐	☐

SECTION 4

Response Readiness

When an incident occurs, the first ten minutes matter most — response readiness is a leadership issue, not just an IT issue.

Question	YES	NO	NOT SURE
10. Do your teams know what to do in the first 10 minutes after a suspicious AI-related request?	☐	☐	☐
11. Do you have a written playbook for deepfake, voice cloning or Shadow AI incidents?	☐	☐	☐
12. Is AI-related risk discussed regularly at management or board level, not only inside IT?	☐	☐	☐

How Ready Are You?

Count your **YES** answers to gauge your readiness level, and use the result as a starting point for an honest conversation with your leadership team.

10–12 YES answers

Strong foundation. Your organisation has solid practices in place. Test them with realistic scenario exercises.

6–9 YES answers

Partial readiness. You have good building blocks, but gaps may appear under pressure. Focus on verification protocols and practical training.

0–5 YES answers

Exposure risk. Your organisation may be vulnerable to AI-powered fraud, Shadow AI and poor decisions under pressure. Start with clear rules and awareness training.

More than 3 NOT SURE answers

Visibility gap. Lack of visibility is a risk in itself. Prioritise understanding your current state before adding new tools.

What Good Preparation Looks Like

AI readiness requires clarity, practice and leadership commitment — not a large budget or a dedicated security team.

Clear AI Usage Rules

Employees should know which AI tools are allowed, what data must never be shared, and who to ask when unsure.

Verification Protocols

Payments, access requests and data transfers should always be verified through more than one channel.

Scenario-Based Training

Leaders and employees need practice with realistic AI scenarios so they know how to respond under pressure.

> When pressure hits, prepared people respond fast.

INFOSHARE 2026 RESOURCE

About This Checklist & Next Steps

This checklist was created by **Joanna Wziątek**, AI Security Strategist, for business leaders attending Infoshare 2026.

It accompanies the keynote session: *"AI-Powered Threats for Business Leaders: A Decision-Maker's Guide."*

For further resources, scenario-based training programmes and executive briefings, visit **www.joannawziatek.pl**

Connect

Joanna Wziątek
AI Security Strategist

joanna@joannawziatek.pl

www.joannawziatek.pl

LinkedIn:
linkedin.com/in/joannawziatek

RECOGNISE. VERIFY. RESPOND.

Discuss AI Readiness

A 15-minute briefing can quickly reveal your biggest gaps and define a practical first step.

Book a 15-Minute Briefing

Schedule directly via Calendly.
calendly.com/kontakt-joannawziatek

Send a Message

Email Joanna to start the conversation.
joanna@joannawziatek.pl

Visit Online

Find resources and event materials online.
www.joannawziatek.pl

Recognise. Verify. Respond.

AI-powered threats target people first, so the best defence is preparation before pressure arrives.

Joanna Wziątek | AI Security Strategist | **joanna@joannawziatek.pl** | **www.joannawziatek.pl** | LinkedIn: **linkedin.com/in/joannawziatek**

Infoshare 2026 Resource — AI Readiness Checklist for Leaders