AI Agent Risk & Readiness Checklist for SMEs

Questions to ask before deploying autonomous AI tools such as OpenClaw

1. Governance & Control

☐ What systems will this AI agent have access to?
☐ Can we limit or control what actions it is allowed to perform?
☐ Does it require human approval before taking important actions?
☐ Can we see what it is doing in real time?
☐ Are detailed activity logs available for auditing and review?

2. Security & Data Protection

☐ Where will our data be stored and processed?
☐ Will any customer or business data be sent to third-party services?
☐ Is the system designed with GDPR considerations in mind?
☐ What encryption or security measures are in place?
☐ Who ultimately controls access credentials and permissions?

3. Reliability & Testing

☐ Has this system been used successfully in real business environments?
☐ Can we test it safely before allowing it access to live systems?
☐ What happens if it makes an error or performs an unwanted action?
☐ Can we easily undo or reverse its actions?
☐ Is there ongoing monitoring to detect problems early?

4. Business Suitability

☐ What specific problem does this AI agent solve for our business?
☐ Could simpler automation or software achieve the same result?
☐ What internal skills are needed to manage this system?
☐ What is the expected return on investment and timeframe?
☐ Will this genuinely save time, or just shift complexity elsewhere?

5. Accountability & Support

☐ Who is responsible if the AI causes financial, operational, or reputational damage?
☐ Is support available if something goes wrong?
☐ Can the AI's decisions be explained if required by clients or regulators?
☐ Is there documentation and guidance for safe use?
☐ Do we have an AI specialist advising us before deployment?

If you cannot confidently answer most of these questions, it is wise to seek advice from an experienced AI consultant before proceeding.

AI can be a powerful asset for SMEs, but only when implemented with the right safeguards in place.