



AI Secure Adoption & Cyber Risk Assessment

AI adoption is accelerating.
We build security in.

AI is no longer limited to a few isolated experiments; it is now embedded in productivity tools, internal applications or agents, and it is also used by suppliers and third parties across the company's ecosystem. Each new integration expands the exposure of sensitive data, access rights and business-critical processes.

The question is no longer simply whether the company uses AI, but where it is already present and, above all, what risks it introduces. This is where organisations need to be equipped to bring AI adoption on the one hand, and its secure adoption on the other, into alignment.

With the **AI Readiness Advisory** and **AI Cyber Risk Assessment**, Orange Cyberdefense turns AI uncertainty into secure adoption decisions by bringing together the capabilities needed to assess, govern, secure and validate AI use.

The first step is to choose the most appropriate pathway. We are here to help clarify the need, define the right scope and select the most relevant next step.



Our promise to you:

Help you move from unclear AI exposure to a prioritised, evidence-based secure-adoption roadmap

AI Readiness Advisory

For clients needing orientation, use-case visibility, ownership clarity or evidence preparation before formal assessment.

Workshop

A short, leadership-oriented workshop to align on AI security priorities, governance questions and the recommended next step.

- Define AI security priorities
- Provide governance and ownership clarity
- Support leadership alignment
- Help decide what to do first

Outputs: AI adoption situation view, priority decisions and recommended next step.

AI Use-case & evidence sprint

A preparation sprint to map AI use cases, ownership, data touchpoints and evidence readiness before selecting the right assessment scope.

- Build AI use-case inventory
- Map owners, tools, data touchpoints and suppliers
- Build an evidence baseline
- Select the right assessment scope or tier definition

Outputs: Use-case inventory, evidence baseline and recommended assessment scope.

AI Cyber Risk Assessment

For clients ready to assess AI-related cyber exposure, control maturity, evidence and remediation priorities.

Essential

- **Scope:** bounded AI adoption, such as Copilot, GenAI productivity tools or a narrow set of use cases.
- **Assessment depth:** baseline review of exposure and key controls across relevant domains.
- **Output depth:** core output pack, focused on top risks and a 90-day action plan.

Assure

- **Scope:** multiple AI use cases within one agreed organisational perimeter.
- **Assessment depth:** structured maturity assessment across the full domain set.
- **Output depth:** full assessment output pack, focused on maturity, findings and prioritised roadmap.

Strategic

- **Scope:** complex, regulated, multi-entity or transformation-led AI adoption.
- **Assessment depth:** expanded assessment of maturity, operating model, dependencies and programme roadmap requirements.
- **Output depth:** expanded assessment outputs, focused on governance and operating-model changes, programme roadmap and investment decisions.

All levels have the same output stack - AI use-case inventory, evidence register, questionnaire and maturity scoring, findings and risk register, assessment report, secure adoption roadmap, and executive readout - and follow the same stepped approach:



Why Orange Cyberdefense?

A cybersecurity leader with global footprint and proven AI security expertise.



From strategy to execution
We help clients go beyond strategy, designing, integrating & operating capabilities end-to-end



Integrated with managed services
We connect consulting to managed security services where evidence and operational readiness support it



Expertise at scale
We bring together the teams, technology, CTI, and partners you need to achieve real results



Cross-sector experience
We deliver to public and private organisations, from mid to large enterprises, across all industries