



Your Secure AI Implementation Partner

Helping defence unlock the value of AI,
securely and responsibly

AI solutions that work with your infrastructure, your data, your rules.

What we deliver



AI-Accelerated Workflows

Automate operations, improve decision-making and efficiency with secure, tailored workflows.



AI-Enabled Solutions

Deploy AI with confidence - scoped, observable, explainable and integrated with your systems.



Assured AI Solutions

Every solution is engineered with data security at its core, incorporating governance and risk controls to ensure alignment with frameworks such as JSP936, ISO/IEC 42001, and NIST AI RMF, from concept through to deployment.



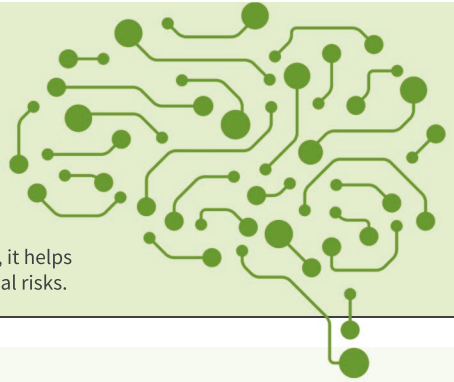
AI-Ready Teams

Empower your workforce with the skills and confidence to use AI effectively. From hands-on training to tailored guidance, we help teams unlock the full potential of AI in secure, high-assurance environments.



Turning AI into a Critical Friend

This prompt example shows how defining context, such as assigning roles to the AI and setting a thinking style, transforms it into a disciplined analytical partner. Rather than generating complete project artifacts, it keeps the human at the center of decision-making. Instead of assuming completeness or accuracy, it helps uncover blind spots, challenge assumptions, and explore potential risks.



1 Assume a role and set the task

You are acting as a Systems Engineer and Site Reliability Engineer (SRE) tasked with analysing interactions and dependencies within the provided system architecture.

3 Challenge assumptions

First, briefly identify and summarise at least two critical areas where provided information is insufficient, ambiguous, overly simplistic, or likely incomplete. Clearly articulate why these gaps or ambiguities could result in emergent, unforeseen, or cascading failures.

5 Complete the task

Only after these gaps have been clarified should you proceed with identifying and detailing emergent risks arising from system interactions. At that stage, explore each emergent risk by clearly addressing:

Interaction & components: what interacts and how.

Risk nature: what can go wrong and why.

Impact & severity: expected effect and justified rating.

Mitigation: concrete actions
(preventive/detective/containment)

1

2

2 Set the thinking style

Operate with critical, independent analysis. Do not assume the provided information is complete and fully captures all relevant interactions—actively look for blind spots, unstated dependencies, ambiguous boundaries or unsupported assumptions.

3

4

4 Propose clarifying questions

Second, propose three specific, targeted questions designed to clarify these gaps. These questions should aim to surface unclear dependencies, assumptions, or potential risks not immediately visible within the documentation. Wait for responses to these questions before proceeding further.

5

6

6 Set style, tone and guardrails

Write in concise British English, neutral. If confidence is low or scope is exceeded, say so and ask follow up questions as required.

Discover more prompt templates and practical tips to maximise your use of AI at <https://www.logiq.co.uk/ai>



INNOVATE. COLLABORATE. DELIVER.

Get in touch for more information.

www.logiq.co.uk/ai
contact@logiq.co.uk
+44 (0)117 457 8120