Is your system a potential elevated risk?

Evaluate potential elevated risk prior to starting the self-assessment as it is used though-out the self-assessment.

Operational impact

Does your system produce or directly influence an administrative decisions (government decision with legal or similar significant effect)?

i.e, automating decisions on issuing infringements.

NO

Operational Impact

Does your system trigger a real-world action with more than negligible potential effect (meaningful change to environment or system state)?

i.e., an automated alerting system.

NO

Autonomous

Does your system operate autonomously or have potential to produce harmful outputs independently of human action, without requiring manual initiation?

i.e., autonomous vehicles.

NO

Data Sensitivity

Was any part of your system trained using sensitive information or can it produce outputs which contain sensitive information?

i.e. a biometric based face matching system.

NO

Unintended harms

Is there a risk of system failure, misuse, or inappropriately deployed that could cause harm to an individual or group?

i.e., systems using unverifiable data inputs.

NO

Explainability and Transparency

Does your system fail to provide explainability for generated content and decisions, hindering comprehension by laypeople and assessment by technical experts?

i.e., information informing policy development

NO

→ **Yes** Yes, to any questions means your use is potentially at elevated risk, and additional mitigation covered in this framework will apply.

→ **No** No to all questions means you are not using AI in a manner which is potentially elevated risk.

ⓘ **Elevated risk**

To determine whether your use is potentially at elevated risk, you will need to make a judgement based on your specific use case. If you are unsure, assume that your use is potentially at elevated risk