GenAI Risk Assessment Template

1. Project Overview

1.1 Guidance: Provide a concise and descriptive title for your project.

Project Title:

1.2 Guidance: Name the individual responsible for the project.

Principal Investigator / Lead Developer:

1.3 Guidance: List the AI tools or platforms you plan to use.

What AI tools are you intending to use:

1.4 Guidance: List the Privacy Policies for the AI tools or platforms you plan to use.

Privacy Policies:

1.5 Guidance: Specify the type user of your project/service/work

Client Type (e.g., Academic, Government, Private Sector, Internal):

1.6 Guidance: Describe the intended use or function of the AI tool.

Purpose of AI Tool:

1.7 Guidance: List any intended AI integrations in the project outputs.

What integrations are you intending to use:

2. Data and Code Sensitivity

2.1 Guidance: Indicate the classification level of the data used.

Classification of Data (e.g. Official, Official Sensitive, Secret, N/A):

2.2 Guidance: State whether the data includes personal information.

Is the data classified as Personal:

2.3 Guidance: Mention any IP or licensing issues related to the data or tools.

Are there any Licensing and Intellectual Property Considerations:

3. Mitigation Measures

4.1 Guidance: Explain how code will be reviewed for quality and security.

Manual Code Review Procedures:

4.2 Guidance: Describe how the AI outputs will be tested and validated.

Testing and Validation Protocols:

4.3 Guidance: Specify how AI-generated code will be documented.

Documentation Standards for AI-generated Code:

4. Intellectual Property (IP) Risks

AI-generated code may inadvertently reproduce licensed or proprietary code fragments, which could lead to IP violations, especially in collaborative or published work. It is essential to assess these risks to ensure compliance with licensing terms, protect proprietary innovations, and maintain the integrity of research outputs.

4.1 Describe any third-party code, libraries, or datasets used in conjunction with the proposed tools:

4.2 Are there any concerns about Copilot-generated code reproducing copyrighted or licensed material?

4.3 If yes or not sure, describe the nature of the concern and any steps taken to verify originality:

4.4 What safeguards are in place to ensure that generated code does not violate IP rights?

4.5 If the project involves publication or external collaboration, describe how IP ownership and licensing will be managed:

Risk Scoring Matrix

Assess each identified risk based on its Likelihood and Impact using a 5x5 scale (1–5). Multiply the two scores to get a Risk Score. Use the color-coded guide below to interpret the score and determine necessary mitigation strategies.

Risk Score Interpretation Guide

Risk Score	Risk Level	Color Code
1–5	Low	Green
6–10	Medium	Yellow
11–15	High	Orange
16–20	Critical	Red
21–25	Severe	Dark Red

Risk Assessment Table

Risk Description	Likelihood (1–5)	Impact (1–5)	Risk Score	Risk Level	Mitigation Strategy

Risk Level Examples

Critical: Use involves personal or classified data. Data governed by high assurance levels. Use directly in business-critical systems or services. Use on a service supporting critical infrastructure, for example power or water systems.

High: Use involves confidential information or business critical information. Security compromise would have a large but limited in scope impact.

Medium: Use on non-critical external facing applications or not used in production but shared information includes production data or config

Low: Model not used in production, no production information shared

Types of risks to Consider

Security: Potential for insecure or vulnerable code generation.

Ethics: Bias, fairness, and accountability in generated content.

Operational: Tool reliability, version control, and auditability.

Compliance: Alignment with STFC, UKRI, and client-specific policies.

Approval and Sign-Off

Name of the risk assessment submitter:

Name of the Theme Leader:

Theme Leader Approval:

Department Head Approval:

Assessment Approval Date: