

Risk Assessment SI

Good Risk Assessment Practices (GRAP)

Version 1.0 | 3 October 2026 | risk-assessment.si

Claudia Otto (COT Legal) | info@risk-assessment.si

To uphold scientific rigour and thus ensure the objectivity essential for objective observability throughout Systems Perceived as Intelligent Risk Assessments (SPAIRA), responsible actors must adhere to best practices, such as the following Good Risk Assessment Practices (GRAP, as amended). They synthesise the Singapore Statement on Research Integrity, the ALLEA European Code of Conduct for Research Integrity, and the U.S. NASEM Framework (Fostering Integrity in Research), as well as derived national consensuses, with established international risk assessment practices, specifically adapted for SPAI. An internationally harmonised version of GRAP is desirable and hereby encouraged.

1. Honesty and objectivity

Risk assessments must be honest and objective. Real-world constraints, such as natural laws, biological realities, and technical limits, must be respected, and must not be arbitrarily denied or subordinated to subjective, science-contradicting, or SPAI-generated claims.

2. Source integrity and transparency

Assessors must maintain honesty regarding the software used and source material, such as literature, third-party expert reports, and other researchers' prior work (whether published or unpublished). Methodologies and methods must be fully disclosed. Conflicting data must not be deliberately omitted, cited inaccurately, or misrepresented.

3. Independence, impartiality, and non-interference

Any conflicts of interest, such as financial, commercial, political, or personal ties that could impair judgement, must be disclosed proactively prior to submitting a proposal, accepting a commission, or commencing the risk assessment. A conflict of roles, such as conducting a risk assessment for one's own risk mitigation or management, that could impair judgement must be disclosed accordingly. The intended use of systems such as SPAI must be disclosed in advance to mitigate the uncontrolled outflow of protected information, as well as foreign manipulation and interference, even if such influence may remain unnoticed by the assessor during the process.

4. Data reliability and rigour

Data collected, produced, and used to assess risks must be valid and representative. Fabrications generated by SPAI must be excluded. Biases among consulted individuals, or within datasets and systems such as SPAI (whether known, hidden, or suspected), must be addressed in accordance with principles 1 to 3.

5. Respect for society and individuals

Assessors must uphold responsibility throughout the process and within (intermediate) findings by accounting for potential physical, non-physical (such as psychological), and societal implications for affected individuals and groups, in particular those who are vulnerable. Anthropomorphisation must be avoided to prevent distortions in the perception of communications during the process and after completion, including, but not limited to, questions and results.

6. Transparency of uncertainty

Epistemic, aleatoric, and other uncertainties (irrespective of their definition) must be communicated in a comprehensible and transparent manner. Where the limits of individual or collective knowledge or feasibility are reached, they must be communicated without ambiguity. The presence of uncertainty and whether or how it affects the results of the risk assessment must be disclosed so as not to impair risk mitigation through, for example, misdirection or the misallocation of resources.

7. Adaptability and professional modesty

Given the fast pace of SPAI development and evolving hybrid threats, risk assessments must not rely exclusively on static assumptions or isolated datasets. Assessors must accept and integrate human and technical fallibility as well as the rapid obsolescence of data, findings, and personal expertise. Where unforeseen aspects exceed their competence, assessors must seek or communicate the need for professional advice or a second opinion without delay, in accordance with principles 2 and 3.

8. Self-correction

If methodological errors, flawed assumptions, or, for example, new or overlooked hazards are identified retrospectively, assessors must review and, if necessary, revise the entire risk assessment process and any (intermediate) findings to ensure that corresponding risks are recognised to enable their mitigation.

9. Open and collegial discourse

Dissenting views and concerns raised, for example, by colleagues must be respected and integrated into the risk assessment process rather than suppressed. Data collection involving experts with diverging views must not be excluded or diminished. Inputs that are dissenting, critical, or broader than the assessor's subjective view must not be altered, truncated, or otherwise reduced in their significance for the results of the risk assessment.

10. Responsible communication

Communication of identified risks to decision-makers, affected parties, or the public must be accurate, complete, and grounded in a risk assessment conducted in accordance with principles 1 to 9. Findings must be contextualised appropriately to prevent misinterpretation. The report must be self-contained, and non-prescriptive regarding subsequent decision-making. Furthermore, communication must neither incite emotions such as fear nor minimise risks for convenience, political alignment, or any other personal advantage, balancing the interest in information with the protection of information as required, including, but not limited to, trade secrets, classified information, and data protection.