AI RISK ASSESSMENT · FIELD NOTES

AI Risk Assessment: A Practical Framework

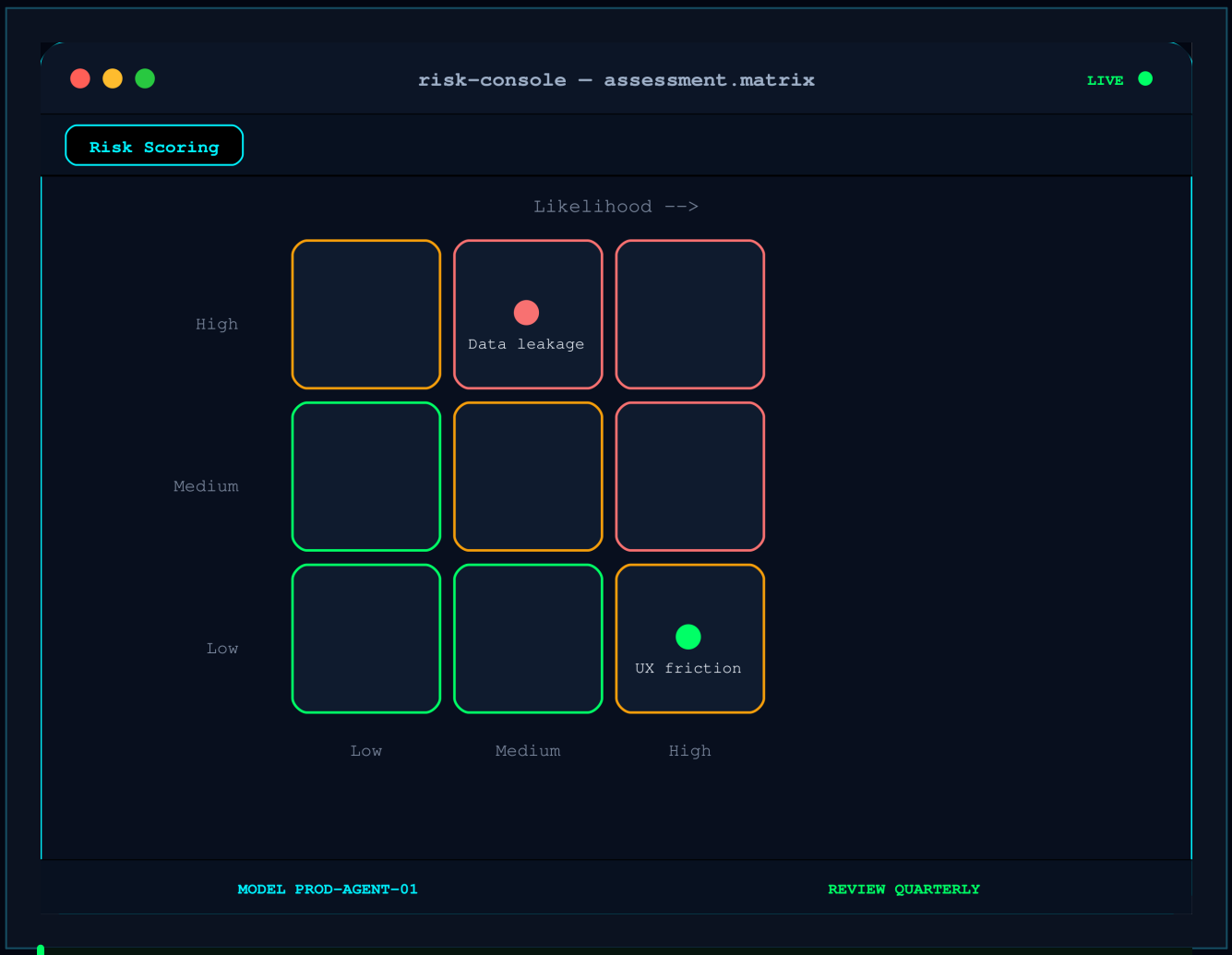
> *“Risk that isn't scored gets handled by whoever is loudest in the room. A shared scoring framework replaces that with a repeatable decision.”*

This dossier is a structured likelihood-times-impact framework for scoring risk in a deployed AI system, so risk decisions are comparable across projects instead of ad hoc.

Scope	Risk scoring methodology for deployed AI systems
Method	Likelihood x Impact matrix, standard risk-management pattern
Output	A ranked risk register, not a single pass/fail verdict
Analyst	Nazline Mwita, Cybersecurity Assurance Lead, HarLyn Digital Partners

1. The Matrix

Every identified risk gets scored on two axes: how likely it is to occur, and how severe the impact is if it does. The combination determines priority — not gut feeling, not whichever risk was raised most recently.



Scoring Principle

High impact, low likelihood still needs a mitigation plan — it does not need panic.

2. Risk Categories Worth Scoring

Data risk: training/context data leakage, unlawful processing, poisoning.

Output risk: hallucination, bias, harmful or non-compliant generated content.

Operational risk: availability, cost runaway, vendor dependency.

Security risk: prompt injection, tool-call abuse, unauthorized access to agent capabilities.

3. Scoring in Practice

Score band	Response
Red (high x high)	Block deployment until mitigated; owner assigned; re-review before launch
Amber (mixed)	Deploy with monitoring and a documented mitigation timeline
Green (low x low)	Accept the risk explicitly — document the decision, don't ignore it silently

4. What This Is Not

It is not a substitute for a real security assessment — the matrix prioritizes what needs review, it doesn't replace the review itself. And a risk register that's never revisited after the initial assessment is a snapshot, not a management tool.

Related Service

This framework underpins the AI Security advisory engagement — turning a general sense of unease about an AI deployment into a ranked, actionable risk register.

Nazline Mwita, CompTIA Security+ certified Cybersecurity Assurance Lead and Co-Founder at HarLyn Digital Partners. Specializing in authorized web & API security assessments, KDPA compliance reviews, and defensive cloud architecture in Nairobi, Kenya.