TOOLKIT - INSTRUMENT 2

Risk Tier Classifier Worksheet

Not every AI use deserves the same level of scrutiny. Use the five factors below to assign a preliminary tier to each system in your inventory, then apply the recommended level of oversight.

Five classification factors

Factor	Question to answer
Consequence	Can the system's output affect a person's rights, benefits, safety, liberty, or livelihood?
Autonomy	Does the output lead to action directly, or does a trained human meaningfully review it first?
Data sensitivity	Does the system process personal, protected, or surveillance-derived data?
Reversibility	If the system errs, how easily can the harm be detected and corrected?
Scale	How many residents does the system touch, and how often?

How to assign a tier

Step 1 - Start with consequence

- No direct resident impact usually points toward Tier 1 or Tier 2.
- Consequential resident impact should generally be treated as at least Tier 3.
- Uses involving liberty, surveillance, biometric identification, coercive enforcement, or serious safety consequences should be considered for Tier 4.

Step 2 - Consider autonomy

- Raise the tier when the output directly triggers action.
- Raise the tier when human review is limited, rushed, procedural, or unlikely to change the result.

Step 3 - Consider data, reversibility, and scale

- Processes sensitive, biometric, protected, or surveillance-derived data.
- May cause harm that is difficult to detect or reverse.
- Affects large numbers of residents, or is used frequently.
- Operates across several departments or services.

Step 4 - Use the higher provisional tier when uncertain

- When a system falls between two tiers, assign the higher provisional tier until legal, technical, privacy, security, and operational review is complete.

The four tiers

Tier 1 - Minimal risk

Typical examples. Internal drafting aids, meeting transcription, internal translation, code assistance, administrative search, and summarization of non-sensitive internal material.

Recommended oversight. Department-level approval, basic acceptable-use rules, staff training, and appropriate records guidance.

Tier 2 - Moderate risk

Typical examples. Resident-facing chatbots, document summarization for public release, service-request routing, permit or application triage, planning analytics, and non-consequential recommendation tools.

Recommended oversight. Responsible-official approval, accuracy testing, a correction pathway, documentation of system limitations, and disclosure when residents interact directly with the system.

Tier 3 - High risk

Typical examples. Systems influencing benefits eligibility, permitting or code enforcement, hiring or employment screening, fraud detection, prioritization of inspections, housing decisions, and access to public services.

Recommended oversight. Enhanced legal, privacy, civil-rights, security, and operational review before deployment; a named human decision-maker; public disclosure; an appeal or correction process; audit logging; and evaluation for potential disparate impacts.

Tier 4 - Critical risk / enhanced review

Typical examples. Policing, surveillance, facial recognition, biometric identification, predictive enforcement, systems affecting liberty, and systems making or strongly determining coercive government actions.

Recommended oversight. Consider whether the use should proceed at all. Apply enhanced legal, privacy, civil-rights, security, technical, and operational review; governing-body authorization where appropriate; public notice and participation; independent evaluation; strict human oversight; incident reporting; and periodic reauthorization.

Worksheet

System	Consequence	Autonomy	Data	Reversibility	Scale	Tier

This template is provided for general informational purposes only and is not legal advice. Each local government should review and adapt it with its own attorney, records officer, privacy, security, and procurement staff.