# W4: LLM solution brief (final deliverable, one page)

How Large Language Models Work: Foundations for Choosing and Applying LLMs at Work (FAST-14) · Lab 4: Grounded assistant and injection test; LLM solution brief

Name: _____ Date: _____

| Section | What to write |
|---|---|
| 1. Task and user | What job the LLM helps with, who uses it, volume per month |
| 2. Approach | Prompt only, RAG, fine-tuning (for example LoRA), or tool use, and why the others were not chosen |
| 3. Model choice | Model type and size, hosted vs local, with evidence (a test like Lab 3) |
| 4. Settings and cost | Temperature or reasoning effort, context needed, estimated monthly cost (show the formula) |
| 5. Data | What data is involved; how Massachusetts personal information (G.L. c. 93H, 201 CMR 17.00) or other sensitive data is kept out or protected; vendor data terms |
| 6. Risks and controls | At least three OWASP LLM Top 10 (2025) risks, each with a matching control; human review points |
| 7. Measures | How you will know it works: a test set, an accuracy target, and who checks |

**Completion criteria**

- The lab test table is complete and the injection result is recorded.
- The brief fills all seven sections.
- The approach choice is justified against the alternatives.
- The cost is shown with a formula.
- At least three OWASP risks are matched to controls.
- No real personal or employer-confidential data appears anywhere in it.