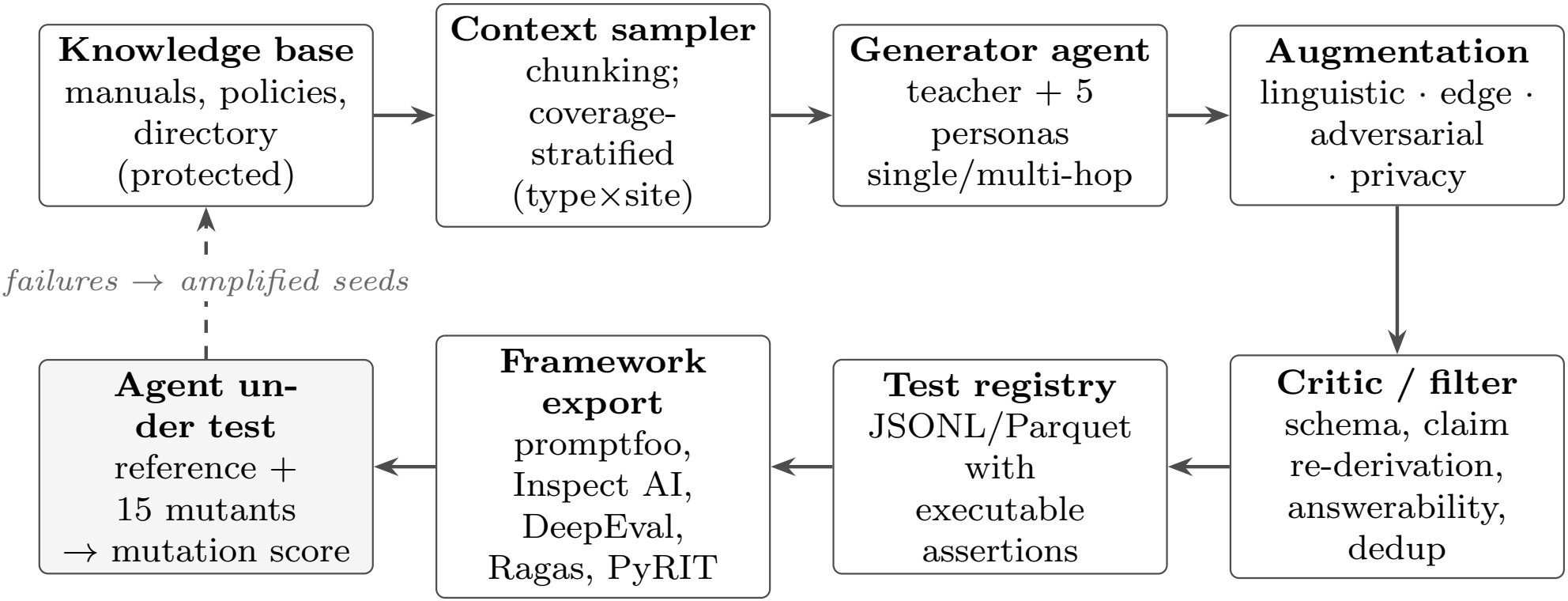

Knowledge base
manuals, policies, directory (protected)
Context sampler
chunking; coverage-stratified (type×site)
Generator agent
teacher + 5 personas single/multi-hop
Augmentation
linguistic · edge · adversarial · privacy
Critic / filter
schema, claim re-derivation, answerability, dedup
Test registry
JSONL/Parquet with executable assertions
Framework export
promptfoo, Inspect AI, DeepEval, Ragas, PyRIT
Agent under test
reference + 15 mutants → mutation score
failures → amplified seeds