AI Readiness Audit

A practical starting point for secure AI adoption

Sample report | Fictional small-business scenario
6 November 2026 | Version 1.0 | Public preview draft

The decision this report supports

Start with a controlled internal knowledge assistant. First fix document ownership and access, then test whether staff can find reliable answers faster. Expand only if the pilot proves useful and the controls hold up.

What a client receives

A plain-language assessment of data, workflows and security; a ranked list of AI opportunities; a risk and control map; and a phased plan explaining what to do first, who owns it, and how to measure progress.

An example, clearly labeled

The company, operating conditions, findings, ratings, costs and targets in this report are hypothetical. No client interviews, system inspections, security tests or pilot measurements were performed. This is a sample deliverable, not a client case study or a claim of achieved results.

The report reflects the fixed-fee, two-week assessment described by Private AI Consulting. Implementation, software, hardware and ongoing support would be scoped separately. No engagement price is implied by this sample.

private-ai.ai
Start small. Prove value. Keep control of your data.

01 / Executive assessment

Illustrative conclusion: ready to prepare a limited pilot; not ready for broad deployment. The business has useful internal knowledge and a clear productivity problem. Its main blockers are inconsistent source documents, untested access boundaries and the absence of an approved AI usage process.

The fictional business

ExampleCo is a fictional Ontario-based technical services company with 35 employees. It uses Microsoft 365, a shared file server, a service desk and a small virtualized environment supported by an external IT provider. Staff repeatedly search for procedures and ask senior colleagues for answers. Client contracts, personnel files and financial records sit outside the proposed pilot scope.

Area	Illustrative readiness	What it means
Business value	Promising	Recurring internal questions offer a narrow, measurable starting point.
Data	Needs preparation	Useful procedures exist, but versions and ownership are inconsistent.
Security and privacy	Conditional	General IT safeguards are assumed; AI-specific permissions and data flows need verification.
Governance and operations	Needs preparation	No approved AI owner, usage policy, evaluation process or support runbook is assumed.

Three actions to take first

1. Name accountable owners. The business sponsor owns value and acceptable risk. IT owns the platform and access. A document owner approves each source. A privacy lead reviews permitted data use.

2. Approve a small document set. Select 100 current, non-sensitive procedures available to every pilot participant. Remove duplicates and assign owners before ingestion.

3. Define the decision gate. Agree the quality, security and value thresholds on page 7 before buying equipment or building a production service.

What this recommendation does not establish

Readiness ratings are qualitative judgments within the invented scenario, not maturity scores or certification results. An actual conclusion depends on interviews, sampled evidence and agreed scope. Unknown or untested controls must remain unverified.

02 / Scope and evidence

A two-week assessment, with a clear boundary

An illustrative engagement covers workflow interviews, a sampled document inventory, architecture and data-flow review, identity and security evidence, use-case selection, and a decision workshop. It is not a penetration test or implementation commitment.

Timing	Assessment work	Client input / output
Days 1-2	Confirm goals, boundaries, and owners; interview sponsor, staff, and IT.	Agreed scope, access, and evidence request.
Days 3-5	Sample workflows and documents; review architecture, access, backups, and current AI use.	Evidence register and preliminary gaps.
Days 6-8	Rank use cases; assess AI risks; compare deployment options and dependencies.	Draft control map and pilot recommendation.
Days 9-10	Validate factual statements with owners; discuss options and next steps.	Final report, action plan, and executive readout.

Timing assumes timely access to agreed people and evidence. A wider scope or delay is handled by agreement.

Evidence labels in this fictional sample

Illustrative: ExampleCo's conditions, ratings, and risks are invented. **Proposed:** Controls, targets, and plans are recommendations, not tested results. **Source basis:** The public service description informs the report format, not ExampleCo findings.

Evidence needed in a real audit

Evidence request	What it would establish
Workflow interviews and timed tasks	Frequency, pain points, and a credible baseline.
Document sample, owners, and access lists	Quality, sensitivity, usage rights, and permissions.
Identity settings and access test results	MFA, joiner/leaver handling, and enforceable boundaries.
Network/data-flow diagrams and provider terms	Where content, embeddings, logs, and backups travel and persist.
Backup restore record, monitoring, and incident procedures	Recoverability and support ownership.

03 / AI use-case priorities

These priorities are illustrative judgments, not measured returns. Value means likely staff benefit; effort includes data preparation and ongoing support. A high-value use case can still be deferred when its data or consequences make it a poor first pilot.

Use case	Value / effort	Risk	Decision and reason
Internal procedure search with source links	High / Medium	Medium	Pilot first. Repeatable questions, bounded sources and reviewable answers.
Draft internal training material from approved procedures	Medium / Low	Medium	Next candidate. Document owners must review every draft.
Draft client proposals using past work	High / Medium	High	Defer. Requires client separation, usage rights and confidentiality controls.
Summarize live client support tickets	Medium / Medium	High	Defer. Tickets may include personal data, credentials and client secrets.
Autonomous changes to business systems	Uncertain / High	High	Exclude from initial work. Broad permissions and errors create operational exposure.

Why internal knowledge comes first

A read-only assistant can show whether AI helps without giving it authority to send messages, change records or make decisions. A curated corpus gives staff a known reference point, makes failures easier to investigate and provides a manageable first evaluation set.

How the actual ranking would be validated

Observe staff completing common tasks. Measure search time and the number of questions that require escalation. Check whether conventional search or a cleaned document library solves the problem at lower cost. Confirm a sponsor, document owner and realistic support capacity before approving AI work.

An illustrative value calculation

Assume 10 users ask 5 questions per day and save 3 minutes per question across 20 working days: 50 staff hours per month. At an assumed CAD 50 per hour, that is CAD 2,500 of potential monthly capacity. These are planning assumptions, not savings evidence; staff capacity is not automatically a cash saving.

Compare measured benefit with licenses, infrastructure, integration, document maintenance, human review and support. Set the spending ceiling before the pilot. This audit does not justify a GPU purchase on its own.

04 / Data, security and privacy

All current-state conditions below are illustrative. The evidence column describes what would be checked before accepting them as real findings.

Data condition assumed	Evidence to check	Required preparation
Procedures have duplicate and outdated versions.	Sample document dates, version history and staff answers.	Approve one current version; assign owner and review date.
Some folders combine general and restricted material.	Inspect access groups and representative file permissions.	Use a dedicated approved collection; exclude restricted material.
PDFs vary in extraction quality.	Compare extracted text with original tables and scanned pages.	Repair or exclude unreadable content; verify source links.
Retention and usage rights are not recorded consistently.	Review retention rules, contracts and document ownership.	Record permitted use and deletion requirements before ingestion.

Security baseline to verify

Review MFA, role-based access, separate administration, patching, endpoint protection, network restrictions, encrypted transport and storage, backups, restore testing and incident escalation. Existing safeguards are useful inputs; they do not establish that an AI service is secure.

Follow the complete data path

Review source files, extracted text, chunks, embeddings, prompts, responses, logs and backups. Treat derived data as potentially sensitive. Identify storage locations, administrators, external connections, retention periods and deletion paths for each. Test ingestion and deletion rather than relying on a diagram alone.

Privacy and permitted use

Start with non-sensitive internal procedures. Exclude client records, employee records, credentials and personal information from this pilot. A named privacy lead must confirm permitted purposes, contractual constraints and any jurisdiction-specific obligations before expanding the scope. This sample makes no legal compliance determination.

Local infrastructure is a control choice

Keeping inference local can reduce external disclosure paths. It does not remove insider access, insecure configuration, malicious documents or sensitive logs. Verify outbound traffic and telemetry. Any external model, OCR service or monitoring integration requires separate approval of data handling, retention and contractual terms.

05 / AI risk and control map

Illustrative inherent risk: High = potential sensitive disclosure or material business harm; Medium = bounded disruption or misleading information. These are scenario judgments before the proposed controls. Residual risk is unverified until tests pass; control presence alone is insufficient.

Risk / rating	Proposed control	Accountable owner	Evidence / release test
R1. Sensitive data leaves the approved environment / High	Approved sources only; default-deny outbound access; review all external services.	IT lead	Data-flow review and traffic inspection show no unapproved transfer.
R2. Users retrieve restricted content / High	Server-side source authorization before retrieval; protect index and direct file links.	IT lead	Negative tests across roles and direct endpoints return no restricted content.
R3. Plausible but incorrect answers / Medium	Source citations, explicit abstention, human checking; no authoritative advice.	Operations lead	Held-out questions meet quality thresholds; sources support the answers.
R4. Instructions hidden in documents / High	Treat documents as untrusted data; no tools or execution; restrict ingestion to approved owners.	IT lead	Adversarial documents cannot trigger actions, reveal secrets or bypass access.
R5. Stale or tampered source material / Medium	Document owners, version records, approved ingestion and removal process.	Document owner	Changed and withdrawn sources update correctly; old answers are retested.
R6. Sensitive prompts or logs persist / High	Minimize logging; role-restrict access; approved retention and tested deletion.	Privacy lead	Inspect logs and backups; test expiry and index/source deletion handling.
R7. Vulnerable components or exposed admin APIs / High	Approved software/model sources, license review, patch process, segmented access and secrets protection.	IT lead	Version register, vulnerability review and endpoint-access tests signed off.
R8. Outage, unexpected cost or poor support / Medium	Usage limits, monitoring, budget ceiling, restore test and manual fallback.	Business sponsor	Load/restore exercise and spend alert work; named operator accepts runbook.

This is a practical control map, not a certification checklist. Record test date, tester, result, exception and owner for every row in an actual engagement. The sponsor accepts documented residual risk only after the responsible owners review the evidence.

06 / Recommended pilot

Proposed pilot: an internal procedure assistant for 10 named users, using 100 approved documents over four weeks after audit closeout. It retrieves relevant passages and drafts answers with source links. It cannot send email, browse external sites, execute commands or change business records.

Deployment recommendation

Begin with a small private deployment if existing supported infrastructure can meet the evaluation needs. Keep the interface, retrieval store, embeddings, model inference and logs inside the approved environment. Use the existing identity provider and encrypted connections. Separate administration from ordinary users. Select a model only after quality, capacity and license checks.

The retrieval service must enforce access before content reaches the model. The first corpus contains only material all pilot users may read. Any future mixed-permission corpus requires additional authorization tests. Restrict direct access to the index and model API; the application login alone is not an access boundary.

Compare options before committing

Local hosting offers direct operational control but requires patching, capacity and support. A managed private service may reduce operations effort but needs approved data handling, location and contract terms. Conventional search remains the baseline. Do not buy dedicated hardware until measured workload and total cost justify it.

Proposed acceptance criteria - not achieved results

Measure	Release / continuation gate
Answer quality	At least 85% of 40 held-out, answerable questions are correct and supported by valid citations, scored by the document owner.
Unanswerable questions	At least 90% of 10 out-of-scope questions produce a clear abstention, without invented instructions.
Security	Zero unauthorized disclosures in at least 20 designed access and injection tests; no unresolved high-risk findings. Passing is limited to tested cases.
Value and cost	At least 20% lower median end-to-end task time, including verification, on matched tasks for the same users; stays within the approved spending ceiling.
Operations	Usage policy accepted; restore, disablement and escalation tested; operator and sponsor sign off.

Use separate tuning and held-out evaluation questions. Record model/configuration versions and failures. Stop access after a suspected disclosure or serious control failure; preserve restricted incident evidence, investigate and retest. If value falls short, improve the sources, narrow the scope or stop the pilot.

07 / Phased implementation plan

These phases are recommendations after the audit, not included delivery promises. The illustrative eight-week sequence depends on staff availability and existing infrastructure. The homepage describes a separate 4-8 week Readiness Sprint; any combined engagement needs its own agreed scope.

Phase	Actions and accountable lead	Decision gate
Prepare Weeks 1-2	Sponsor names owners and budget. Operations approves sources. IT validates baseline and data flows. Privacy lead approves permitted use.	Proceed only with a signed pilot charter, approved corpus and no unresolved blocking control gaps.
Build and evaluate Weeks 3-4	IT configures an isolated, read-only service. Document owner builds evaluation questions. IT tests access, logging, injection resistance and recovery.	Release to named users only when pre-release controls and quality checks pass.
Run pilot Weeks 5-6	Operations collects task timings and user feedback. IT monitors incidents, capacity and spend. Document owner reviews failures weekly.	Sponsor reviews all page 7 measures and decides: stop, revise or proceed.
Harden or close Weeks 7-8	If approved, IT assigns service ownership, change control and support. If stopped, remove access and derived data under the retention plan.	Expand only after evidence-backed approval. Each new source, user group or capability triggers reassessment.

The first-week action list

Business sponsor: approve purpose, participants, budget ceiling and acceptable risk.
Operations lead: select the 100-document collection and record task-time baseline.
IT lead: document the data path, test identities and confirm capacity.
Privacy lead: approve exclusions, retention and any third-party handling.
Document owner: approve current sources and evaluation answers.

Scope of a follow-on proposal

Confirm deliverables, responsibilities, access requirements, acceptance criteria, exclusions, fees and operating costs before work begins. Implementation and continuing support remain separate from the fixed-fee audit. The client retains the report and can act on the recommendations without a further engagement.

What the sponsor should approve now

Approve the preparation phase and evidence collection. Defer a production rollout, autonomous actions and a hardware commitment until the pilot provides a defensible reason to proceed.

08 / About this illustrative sample

This is a preview of the format and level of advice an AI Readiness Audit could provide.

ExampleCo is fictional. Its company profile, operating conditions, findings, risk ratings, cost assumptions, targets, and timelines were created for this example. No client interview, system inspection, security test, or pilot measurement was performed for ExampleCo.

What the sample demonstrates

- A plain-language decision: prepare, pilot, revise, or defer.
- A distinction between checked evidence, assumptions, proposals, and unknowns.
- A review of data, workflow, access, privacy, security, and operating questions before implementation.
- An action plan with owners, dependencies, and measures for a later pilot decision.

How a real engagement would differ

A real audit begins with an agreed scope and authorized access to people and evidence. Its report identifies which statements were verified, the evidence and sampling limits, the responsible owners, and what remains untested. Findings and recommendations would reflect that client's actual systems and constraints.

Scope and status

This preview is a draft, not a client case study, certification, penetration test, legal opinion, or proof of achieved results. The final assessment scope, fee, schedule, and any follow-on technical work are agreed separately with each client. The sample may change as the service material is refined.

private-ai.ai | Discuss an AI Readiness Audit