SMALL-BUSINESS FIELD GUIDE · EDITION 2026-10-09.1

One useful task. One honest test.

A practical workshop for drafts you can check. Six original worksheets, a worked example, and a decision to keep, change or stop. No invented success stories.

Educational edition. Independent specialist review and reader testing remain pending. Hypothetical examples are not business evidence.

> **Start with a low-risk draft, not a live decision.**
>
> Do not begin with payments, hiring, health, legal advice or information you cannot safely share. Prompts do not enforce permissions. In this guide, a person checks and sends the result manually.

WORKERS & BUSINESS OWNERS · 15-MINUTE EXERCISE

Task-to-Test Planner

A bounded experiment for one recurring task — not a prediction about your job.

> **When not to use it**
>
> Do not start with payments, hiring decisions, clinical advice, legal conclusions, or work you cannot independently check.

1. Name one task and the person who uses its output. Be more specific than “write reports”.
2. Describe the bottleneck: too many inputs, unclear instructions, repetitive drafting, or decisions that need expertise.
3. Choose one draft or organising step. Keep the final decision with a person.
4. Write three observable acceptance criteria and one stop condition.
5. Compare with your normal process, including setup, checking and correction time.

WORKED EXAMPLE · HYPOTHETICAL

Hypothetical workshop: draft a reply about opening hours from a public FAQ. It must preserve the exact hours, not invent prices, and flag questions the FAQ does not answer. A staff member reviews the reply and sends it manually. Stop if a trial invents a commitment or a fact.

Your worksheet

No confidential information. Filling this sheet does not send data to an AI provider. Blank prompts can be copied separately.

Task and intended reader

Current process and bottleneck

Approved inputs (no confidential data)

One AI-assisted step

Three acceptance criteria

Reviewer, stop condition and fallback

▼ **Optional prompt · use only approved inputs**

Help me test one recurring task. Ask what result is needed, what approved inputs exist, what mistakes matter, and who can check the output. Suggest one bounded draft step or say AI is unsuitable. Produce three acceptance criteria, a stop rule and a manual fallback. Do not invent facts, savings or a job-risk score. Do not request sensitive records.

Using this prompt in another service sends your inputs to that service. Check its settings first. It is not a tested guarantee of output quality.

Before you use the result

- Can a reviewer check every important output against an approved input?
- Is the test reversible and separate from live actions?
- Would the experiment still be useful if the result were “do not use AI”?

ANYONE BRIEFING AN AI TOOL · 15-MINUTE EXERCISE

Context and Boundaries Card

A handover that explains what matters, what is unknown, and what must not happen.

> **When not to use it**
>
> Do not include passwords, client identifiers, private relationship histories or culturally restricted knowledge.

1. State the outcome and audience. Specify what this task does not cover.
2. List the authoritative documents with version dates and owners.
3. Explain the operational reason for important rules, not just the rules themselves.
4. Separate facts, assumptions and unanswered questions.
5. Name the reviewer and actions requiring permission. Set a review date for the card.

WORKED EXAMPLE · HYPOTHETICAL

Hypothetical workshop: the FAQ lists Tuesday–Saturday, 9 am–4 pm. Holiday hours are not confirmed. The tool must say “please contact the team” for holidays, not infer them from a general calendar. Sending the reply remains a staff action.

Your worksheet

No confidential information. Filling this sheet does not send data to an AI provider. Blank prompts can be copied separately.

Outcome, audience and exclusions

Approved sources, versions and owner

Rules and why they exist

Known facts / assumptions / unknowns

Forbidden actions and approvals

Reviewer and next review date

▼ Optional prompt · use only approved inputs

Turn my non-sensitive notes into a task handover. Organise outcome, approved sources, constraints, unknowns, prohibited actions and human approvals. Keep assumptions visibly separate from facts. Ask about missing rules instead of inventing them. A prompt is guidance, not a security control; identify which restrictions need actual permissions.

Using this prompt in another service sends your inputs to that service. Check its settings first. It is not a tested guarantee of output quality.

Before you use the result

- Does an outsider know which document wins if sources conflict?
- Are unknowns explicit rather than filled with plausible guesses?
- Are permissions enforced outside the prompt where necessary?

ANYONE REVIEWING AI OUTPUT · 15-MINUTE EXERCISE

Output Check Lab

A reusable acceptance-test sheet and practice spotting plausible mistakes.

> **When not to use it**
>
> Do not treat a second AI agreeing with the first as independent verification, or use these exercises to approve high-stakes advice.

1. Choose the actual decision the output supports.
2. For each important claim, name the source a reviewer can check.
3. Create a normal case, a missing-information case and an exception case.
4. Check for omissions, invented commitments, incorrect calculations and unsupported recommendations.
5. Reject or revise failures. Repeat the checks after revision and record what still needs a specialist.

WORKED EXAMPLE · HYPOTHETICAL

Hypothetical workshop: approved FAQ says opening hours only. An AI reply says “we are open 9–4 and delivery is always free”. The hours may pass; “always free” must fail because no delivery policy was supplied. Fluent prose does not make the extra promise true.

Your worksheet

No confidential information. Filling this sheet does not send data to an AI provider. Blank prompts can be copied separately.

Output purpose and decision

Authoritative inputs

Normal case and expected result

Missing-information case and expected result

Exception case and expected result

Fail conditions and reviewer

▼ Optional prompt · use only approved inputs

Review this draft against only the approved inputs I provide. Return a table: claim or omission, supporting input, pass/fail/unknown, and correction. Flag unsupported claims even if plausible. Do not manufacture citations. Do not call the work safe or compliant. Suggest tests for normal, missing-information and exception cases.

Using this prompt in another service sends your inputs to that service. Check its settings first. It is not a tested guarantee of output quality.

Before you use the result

- Does every pass have a traceable reason?
- Are omissions checked as well as sentences that are present?
- Is the cost of a wrong answer reflected in who reviews it?

SMALL TEAMS DECIDING WHETHER TO CONTINUE · 20-MINUTE EXERCISE

Pilot Decision Sheet

A keep, change or stop decision supported by your own observations.

> **When not to use it**
>
> Do not extrapolate from one successful draft to all work, or count faster generation as net time saved.

1. Choose a fixed batch of representative, low-risk tasks. Record the usual time and quality.
2. Measure briefing, generation, checking and correction separately. Include setup and tool charges.
3. Record mistakes by consequence, not just count. Protect the trial from customers and live actions.
4. Ask staff whether the new process creates extra work elsewhere.
5. Compare observed quality and total effort. Keep, change or stop; choose a date to review the decision.

WORKED EXAMPLE · HYPOTHETICAL

Hypothetical arithmetic, not a claimed business result: 10 drafts normally take 12 minutes each. A trial needs 40 minutes setup plus 3 minutes drafting, 4 checking and 2 correcting per draft: 130 minutes total versus 120 normally. Faster drafting did not save time on this batch.

Your worksheet

No confidential information. Filling this sheet does not send data to an AI provider. Blank prompts can be copied separately.

Task batch and baseline

Setup time / per-task draft, check and correction time

Tool and maintenance costs

Failures and consequences

Staff/customer effects and reviewer

Keep / change / stop, reason and review date

▼ Optional prompt · use only approved inputs

Help me compare a limited trial with its baseline. Use only my measured inputs. Include setup, review, correction and tool costs. Show the calculation, missing evidence and quality failures. Recommend keep, change or stop with conditions. Do not invent ROI, future savings or customer outcomes.

Using this prompt in another service sends your inputs to that service. Check its settings first. It is not a tested guarantee of output quality.

Before you use the result

- Are baseline and assisted tasks comparable?
- Is checking and rework included?
- Would a serious quality failure override a time saving?

Small-Business AI-Use Starter Policy

An editable operational policy to discuss with your team — not a compliance certificate.

> **When not to use it**
>
> Do not adopt this unchanged for health, legal, finance, employment decisions or other regulated work. Determine applicable law and seek qualified advice.

1. List approved tools, accounts, owners and permitted low-risk uses.
2. Create a never-enter list and clarify approved data settings.
3. Keep a named person responsible for factual checks and final publication.
4. Require separate approval for external messages, payments, deletions and access changes.
5. Tell staff how to report a mistake without blame. Set a review date and update after incidents.

WORKED EXAMPLE · HYPOTHETICAL

Editable starter: “We use [approved tool] to draft from [approved non-sensitive sources]. Do not enter credentials, client identifiers, health information or confidential files. [role] checks facts and approves publication. No AI tool may send, pay or delete without separately configured approval. Report mistakes to [contact]. Review on [date].”

Your worksheet

No confidential information. Filling this sheet does not send data to an AI provider. Blank prompts can be copied separately.

Policy owner, scope and review date

Approved tools and permitted uses

Never-enter information and data settings

Output review and disclosure rules

Permissions, payment checks and incidents

Training, applicable obligations and escalation contact

▼ Optional prompt · use only approved inputs

Help draft an operational AI-use policy from my approved tools and low-risk uses. Include prohibited data, human review, actual permission controls, staff training, incident handling and a review date. Keep placeholders for missing facts. Flag legal questions for qualified review; do not certify compliance or assume the Privacy Act applies identically to every business.

Using this prompt in another service sends your inputs to that service. Check its settings first. It is not a tested guarantee of output quality.

Before you use the result

- Can staff identify the approved account and never-enter list?
- Are actual access controls separate from policy wording?
- Have applicable obligations and exceptions been checked?

Provider Exit Checklist

A tested record of what you can recover, reuse and revoke.

> **When not to use it**
>
> Do not equate “export available” with portable behaviour, or self-hosting with automatic privacy and reliability.

1. Inventory documents, instructions, decision records, integrations and provider-held memory.
2. Attempt a non-sensitive export. Record its format and whether another tool can use it.
3. Separate your source records from model-specific summaries, embeddings and hidden state.
4. Rehearse revoking access and doing the task manually. Check retention and deletion terms.
5. Record verified, unverified or unavailable for each capability. Review after terms or pricing changes.

WORKED EXAMPLE · HYPOTHETICAL

Hypothetical workshop: a team can export its FAQ and task briefs as plain text, but cannot recreate an assistant’s undocumented preferences. Keeping owned source documents makes switching easier; it does not guarantee identical output from another model.

Your worksheet

No confidential information. Filling this sheet does not send data to an AI provider. Blank prompts can be copied separately.

Dependencies and owner

What exports / format / test date

What does not transfer

Access revocation and manual fallback

Retention, deletion and pricing questions

Verified / unverified / unavailable, next action

▼ Optional prompt · use only approved inputs

Audit my dependency on this service using only evidence I provide. Separate documented export rights from capabilities actually tested. List what may not transfer, access revocation, retention questions, switching effort and a manual fallback. Use verified/unverified/unavailable. Do not invent contract terms, legal clauses or guarantees of portability.

Using this prompt in another service sends your inputs to that service. Check its settings first. It is not a tested guarantee of output quality.

Before you use the result

- Have you attempted the export, not just read a marketing claim?
- Can someone find the original rules without the provider?
- Does the fallback work if the service is unavailable today?

A week that produces evidence

1	Choose one low-risk task and its reviewer. Complete the task and context cards.
2	Write normal, missing-information and exception tests before opening the tool.
3	Use public or invented inputs. Compare with the usual process and record all effort.
4	Review every important result. A serious failure means stop and revise the workflow.
5	Decide keep, change or stop. Set a review date and retain a working manual alternative.

This is a suggested sequence, not a promised completion time or an adoption deadline. Move at the pace your evidence and safeguards allow.

Sources & scope

Edition 2026-10-09.1. AI-assisted editorial revision; independent specialist and reader review pending. Educational material, not legal, medical or financial advice. Examples are hypothetical unless explicitly documented.

- OAIC: privacy and commercially available AI products ↗ (https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-the-use-of-commercially-available-ai-products)
- OAIC: when the Privacy Act covers a small business ↗ (https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/small-business)
- OAIC: automated-decision transparency, commencing 10 December 2026 ↗ (https://www.oaic.gov.au/news/media-centre/new-resources-on-transparency-for-use-of-ai-and-automated-decision-making)
- ASD: small-business cyber security guidance ↗ (https://www.cyber.gov.au/learn-basics/explore-basics/small-business)

HOW WE PUBLISH AND CORRECT → (/EDITORIAL)