



A GUIDE FOR PHILIPPINE SMALL BUSINESSES

A Practical Guide to AI

How to start safely, solve one real problem and know whether it worked.

**Start with the work,
not the technology.**

One task. One owner. One measure. One clear reason to stop.

AI-first looked promising. Data-first proved more useful.

FROM AGPT'S EXPERIENCE

AGPT began, as many firms do, by looking at what AI could do. The more useful lesson came later: a business should not become AI-first. It should become data-first.

If records are scattered, responsibilities are unclear or nobody checks the result, a powerful tool can make confusion spread faster. If the process is understood and the information is reliable, even a modest tool can help.

The right first step may be AI. It may also be digitizing records, improving a process, using ordinary automation or deciding not to proceed.

99.63%

of Philippine establishments in PSA's 2023 List of Establishments were MSMEs.

Basic digital access was common in 2021: 90.8% of establishments owned and used computers and communication equipment, and 81% had internet access. A separate PIDS establishment survey put the overall AI adoption rate at 3.02%.

Sources: PSA 2023 List of Establishments, as presented by DTI; PIDS DP 2024-35, using 2021 PSA SICT and PIDS SIA data.

PIDS also reports 14.9% in its FIRE technology-use findings. The 3.02% used here is the paper's defined overall adoption rate across establishments.

This guide begins at that real starting point. It does not begin with the latest technology.

One chat order. Five different kinds of help.

Imagine a customer sends an order through chat.

- 1** Digitization
Put the order into a usable business record instead of leaving it in a message thread.
- 2** Automation
Follow a fixed rule: when an approved order is due tomorrow, send a reminder.
- 3** AI assistance
Turn the message into a draft order or prepare a reply. A person checks it.
- 4** AI agent
Take several connected steps using other tools. Because it can act, it needs narrow permissions, logs, limits and approvals.
- 5** Augmentation
Help a person perform the work. It improves human judgment without hiding responsibility.

Which part of this work needs help, and what is the simplest safe way to provide it?

Four changes worth watching. Not every new model.

01

AI is becoming a feature

Writing, search, accounting and customer tools increasingly include AI. Check what existing systems can do before buying another one.

02

More than text

AI can interpret documents, images and audio. This can help with extraction, transcription and drafting. A person still needs to check the output.

03

Approved information

A tool can answer using an approved product list, policy or knowledge base. This can make answers more useful, but a person still needs to check them.

04

Agents can act

Promising, but a poor first project for many small firms. Start with assistance. Give authority only when the work and controls are mature.

Practical response

Use the smallest useful capability. Do not let a product roadmap set your business priorities.

Begin with evidence of friction.

- ✓ Customers wait.
- ✓ Staff repeat the same step.
- ✓ Information is typed more than once.
- ✓ Errors or rework recur.
- ✓ The owner cannot see what is happening.
- ✓ Follow-ups are missed.
- ✓ Decisions wait for scattered information.

USEFUL PROBLEM STATEMENT

“Orders are delayed because details arrive in several message threads.”

TOO EARLY

“We need an AI chatbot.”

A stronger first task is:

Frequent

Happens enough to matter.

Defined

The result is clear.

Supported

Usable information exists.

Reviewable

A person can check it.

Recoverable

A mistake can be corrected.

Choose a problem whose improvement would be visible within a month.

Know your starting position.

What work looks like today

Best next move

Manual and scattered

Paper, chat threads, separate files

Capture the minimum useful records. Use a practical digital system that fits the business.

Digital but inconsistent

Different fields, names and owners

Standardize the information and workflow.

Stable and rule-based

A clear condition determines the action

Use ordinary automation.

Organized and judgment-heavy

Language, extraction or patterns matter

Test AI assistance with human review.

Connected and governed

Reliable systems and controls already work

Consider integration, custom AI or a controlled agent.

More technology is not always progress. A clean order record may create more value than a new AI tool.

Map the process before choosing software.

- 1 What starts the work?
- 2 What information arrives?
- 3 Who performs each step?
- 4 Which rule or judgment is used?
- 5 What record changes?
- 6 Who approves the result?
- 7 What happens when something is unusual?

Information check

- ✓ Complete enough for the task
- ✓ Current
- ✓ Names, dates, units and categories are consistent
- ✓ One business-owned source
- ✓ Lawfully available for this purpose
- ✓ Access limited to people who need it
- ✓ Backed up with a retention rule

Data-first does not mean collect everything. Keep the minimum reliable information needed to do the chosen task well.

Use the smallest intervention that works.

1

Process fix

Remove an unnecessary step or agree on one form.

2

Digitization

Capture activity in a usable, business-owned record.

3

Ordinary automation

Apply a stable “if this, then that” rule.

4

AI assistance

Draft, summarize, extract, classify or suggest; a person decides.

5

Controlled agent

Connect steps with strict permissions and approvals.

6

Custom system

Build only when the need is strategic and worth ongoing support.

Default: try an approved feature in a tool you already use; prefer assistance before autonomous action.

Orders arriving through chat

Present situation

A small retailer receives Messenger and Viber orders. Staff copy details into a notebook and ask customers to repeat missing information. Some orders are delayed.

First improvement

Use one approved order form and one business-owned record. Agree on product names, quantities and delivery fields.

Possible AI pilot

Let an assistant turn a message into a draft order and flag missing details. A staff member compares it with the message and confirms it before stock changes.

MEASURE

Time to prepare an order, missing fields and corrections.

WHEN TO STOP

Pause if the tool invents a product or quantity, exposes another customer's data, or changes stock without approval.

The value comes from the whole process, not from the draft alone.

Preparing a client proposal

Present situation

A professional-services firm spends hours on first drafts. Staff repeatedly search for approved descriptions, scope language and standard terms.

First improvement

Maintain one approved library of services, qualifications, exclusions and terms.

Possible AI pilot

Create a first draft from a structured client brief and the approved library. The engagement owner verifies facts, price, scope and commitments before anything leaves the firm.

MEASURE

Drafting time plus review and correction time; factual errors and unapproved commitments.

WHEN TO STOP

No confidential material in an unapproved account, invented credentials or sending without approval.

AI can help prepare the first draft. A person remains responsible for every promise made to the client.

Making an inventory decision

Present situation

A food business runs out of fast-moving items while slow-moving items remain unsold. Sales and inventory records use different names.

First improvement

Standardize item codes, units and stock adjustments. Reconcile the records.

Possible pilot

Begin with a simple reorder rule. If seasonal or irregular patterns make that inadequate, test an AI recommendation. Keep purchase approval with a person.

MEASURE

Stockouts, expired or slow stock, emergency purchases and preparation time.

WHEN TO STOP

No automatic buying. Flag unusual demand. Revert if records are incomplete.

Better data and ordinary automation may outperform AI.

Choose the right risk level for this use.

LOW RISK

Small internal test

Low-risk brainstorming, approved internal drafting, summarizing approved documents and reviewable classification. Use an approved account and check the output.

CAUTION

Stronger safeguards needed

Customer or public content, internal financial or employee information, recommendations, transcription, system connections or agents preparing records. Document, restrict, test, approve, log and maintain fallback.

HIGH RISK

Specialist help first

Payments or credit; employment decisions; health, legal, tax or safety advice; sensitive data at scale; significant profiling; filings; biometrics; or uncontrolled authority to buy, pay, delete, publish or send.

The risk depends on how the tool is used, not which company made it.

Five safeguards every pilot needs.

Privacy

Enter only information approved for the task. Know what the provider receives, retains and uses.

Security

Use business accounts, strong sign-in protection, minimum access, backup and fallback.

Accuracy

Check facts, calculations, names, dates, citations and instructions against a reliable source.

Ownership

Protect confidential material. Check copyright, provider terms and business contracts.

Transparency

Decide what should be disclosed and how people can question or correct an output.

AI can produce plausible but false material.

Personal data remains the business's responsibility. Philippine privacy obligations apply when AI systems process personal data, including during deployment, training and testing.

Reference: National Privacy Commission Advisory No. 2024-04.

Follow these safeguards every time the tool is used.

Keep a person accountable.

“Human in the loop” is too vague. Name the person and the decision.

The owner

- ✓ Approves the purpose and permitted information
- ✓ Decides who may use it
- ✓ Confirms the review point
- ✓ Watches the measure and incidents
- ✓ Chooses continue, change or stop
- ✓ Retires access when the use ends

Employees

- ✓ Know which tools are approved
- ✓ Know what information is prohibited
- ✓ Check the required outputs
- ✓ Report mistakes and incidents
- ✓ Use the fallback when needed

A faster first draft that creates more review work is not an improvement.

Include the people who perform the work when mapping the process and testing unusual cases. They often know where problems are likely to happen.

Write the pilot on one page.

Problem

What result is not good enough today?

Task

What single part will change?

Owner

Who is responsible?

Users and data

Who may use it? What is permitted?

Starting result

What happens under the old method?

Test cases

Normal, difficult, prohibited and failure.

Human check

Who approves an important output?

Fallback

How will essential work continue?

Limits

Time, users, volume and spending.

When to stop

Which error or incident ends the test?

Decision date

When will the business decide?

Decision

Continue, change, stop or escalate.

A useful pilot is deliberately small: one task, a few trained users, approved sample information before live information, two to four weeks, and no high-impact action without approval.

Do not test only the perfect example.

NORMAL

The common task

The request the tool should handle correctly and consistently.

DIFFICULT

The unusual task

Missing, contradictory or unusual information; Taglish, spelling differences or unsupported requests.

PROHIBITED

Outside authority

Personal, confidential or harmful information; an action the tool must reject or escalate.

FAILURE

When service breaks

No internet, unavailable service, incorrect output or broken system connection.

Sometimes the correct result is “ask a person,” “do not proceed” or “use the manual process.”

Keep examples of important errors. They become future tests and training material. Safety improves when the business knows the limits and can recover.

Measure value honestly.

**Estimated monthly value = verified time value saved +
avoidable error cost reduced + other verified benefit –
subscription – review – support – added operating cost**

Measure the result

- ✓ Minutes per task
- ✓ Response or completion time
- ✓ Errors and corrections
- ✓ Missed transactions
- ✓ Review and rework time
- ✓ Stock, collections, complaints or exceptions

Count the full cost

- ✓ Subscription
- ✓ Setup and integration
- ✓ Training
- ✓ Checking and correction
- ✓ Internet and equipment
- ✓ Outside support and maintenance
- ✓ Incident or interruption cost

Continue

Result improved
and controls
worked.

Change

Opportunity
remains, but the
method needs work.

Stop

Improvement is
insufficient or risk is
unacceptable.

Escalate

Integration or
specialist
assessment is
needed.

Cloud, local or hybrid?

Cloud

Usually faster to start and easier to maintain. Provider dependence, internet, current terms and recurring fees matter. Understand where information goes and how to export it.

Local

Can offer more control, but needs capable people, equipment, updates, security, backup and support. Local does not automatically mean secure or inexpensive.

Hybrid

Keeps sensitive records in controlled systems while approved cloud services handle limited tasks.

Ask every supplier

- ✓ What information do you receive?
- ✓ Is it used for model training?
- ✓ Where is it stored and for how long?
- ✓ Can we limit access and review activity?
- ✓ Can we export our information?
- ✓ What happens when the service ends?

Choose based on the task, information, risk, support capacity and total cost. Do not choose based on a slogan.

When an agent is appropriate, and when it is not.

Use an agent only when a simpler automation or assistant is inadequate.

Narrow authority

- ✓ One narrow task
- ✓ Approved sources and tools
- ✓ Smallest permissions
- ✓ Activity logs
- ✓ Simulation before live access

Hard boundaries

- ✓ Approval for external or material actions
- ✓ Spending, time and volume limits
- ✓ Duplicate-action protection
- ✓ Clear escalation route
- ✓ Kill switch and fallback

APPROVAL GATE

No sending, paying, buying, deleting, publishing or material record change without the stated approval.

Authority must be earned through evidence and controls.

Your next 30 days.

01

Choose

Select one task. Map the work. Record the starting measure. Name the owner and reviewer.

02

Prepare

Clean the minimum information. Choose the smallest intervention. Set permitted data, test cases and the conditions for stopping.

03

Test

Use a few trained people and a small volume. Review important outputs. Record time, rework, errors and incidents.

04

Decide

Compare the old and new methods. Count full cost. Continue, change, stop or escalate.

Start small enough to learn, but measure seriously enough to decide.

AGPT can help establish reliable information, disciplined processes and a controlled path from digitization to appropriate automation or AI.

This guide is general information. It does not replace legal, privacy, cybersecurity, tax, employment or sector-specific professional advice.

Where this guide gets its information.

1. **Philippine Statistics Authority**
2023 List of Establishments, as presented in DTI's 2023 Philippine MSME Statistics in Brief
2. **Philippine Statistics Authority and Department of Information and Communications Technology**
2024 National ICT Household Survey
3. **Philippine Institute for Development Studies**
Readiness for AI Adoption of Philippine Business and Industry
4. **World Bank**
Philippines Growth and Jobs Report 2025
5. **National Privacy Commission**
NPC Advisory No. 2024-04
6. **NIST**
AI Risk Management Framework and Generative AI Profile
7. **OECD**
AI Adoption by Small and Medium-sized Enterprises
8. **UK DSIT**
AI Adoption Research
9. **Australian Government**
Artificial Intelligence for Business
10. **UK NCSC**
Small Business Guide to Cyber Security

Philippine learning cases

Asian Development Bank Digital Sandbox page on the SukiPlus pilot and alternative credit scoring for sari-sari stores; Konrad-Adenauer-Stiftung on manufacturing SME adoption in Southeast Asia; International Labour Organization on the digital novice enterprise.

The guide's data-first position reflects AGPT's own experience exploring AI initiatives. It is an experience statement, not a measured case study.

Scenario note: The three business stories in this guide are illustrative scenarios. They are not AGPT clients, survey responses or measured case results.

Direct links and full citations are maintained in the approved manuscript and website version.

