

Local First, AI Second

A Practical Guide to Private Models for Sensitive Work

Ngo Trung Kien

Contents

Copyright and publication notice	1
Introduction: the promise and the boundary	3
Visual frontispiece	4
0.1 Who this book is for	4
0.2 Thesis and falsification condition	4
1 Define the Boundary Before the Model	7
1.1 In plain terms	7
1.1.1 Chapter contract	7
1.2 The decision at stake	7
1.3 Working model	8
1.3.1 See the chapter in practice	8
1.3.2 Chapter-specific operating protocol	10
1.3.3 Operating workflow	12
1.3.4 Evidence and control graph	13
1.4 Worked composite case file — illustrative, not empirical evidence	14
1.4.1 Scenario trace	15
1.4.2 Artifact handoff	16
1.4.3 Evidence application	16
1.4.4 Transfer test	16
1.5 Measurement and recovery decision	16
1.6 Practice lab	17
1.7 Limits and judgment	17
1.8 Takeaways	18
1.9 Reflection	18
2 Classify the Workload	19
2.1 In plain terms	19
2.1.1 Chapter contract	19
2.2 The decision at stake	19
2.3 Working model	20
2.3.1 See the chapter in practice	20
2.3.2 Chapter-specific operating protocol	22
2.3.3 Operating workflow	24
2.3.4 Evidence and control graph	25
2.4 Worked composite case file — illustrative, not empirical evidence	26
2.4.1 Scenario trace	27
2.4.2 Artifact handoff	28
2.4.3 Evidence application	28
2.4.4 Transfer test	28

2.5	Measurement and recovery decision	28
2.6	Practice lab	29
2.7	Limits and judgment	29
2.8	Takeaways	30
2.9	Reflection	30
3	Right-Size Hardware and Models	31
3.1	In plain terms	31
3.1.1	Chapter contract	31
3.2	The decision at stake	31
3.3	Working model	32
3.3.1	See the chapter in practice	32
3.4	Illustrative memory-sizing worksheet	34
3.4.1	Chapter-specific operating protocol	34
3.4.2	Operating workflow	36
3.4.3	Evidence and control graph	37
3.5	Worked composite case file — illustrative, not empirical evidence	38
3.5.1	Scenario trace	39
3.5.2	Artifact handoff	40
3.5.3	Evidence application	40
3.5.4	Transfer test	40
3.6	Measurement and recovery decision	40
3.7	Practice lab	41
3.8	Limits and judgment	41
3.9	Takeaways	42
3.10	Reflection	42
4	Verify Model Provenance and Terms	43
4.1	In plain terms	43
4.1.1	Chapter contract	43
4.2	The decision at stake	43
4.3	Working model	44
4.3.1	See the chapter in practice	44
4.3.2	Chapter-specific operating protocol	46
4.3.3	Operating workflow	48
4.3.4	Evidence and control graph	49
4.4	Worked composite case file — illustrative, not empirical evidence	50
4.4.1	Scenario trace	51
4.4.2	Artifact handoff	52
4.4.3	Evidence application	52
4.4.4	Transfer test	52
4.5	Measurement and recovery decision	52
4.6	Practice lab	53
4.7	Limits and judgment	53
4.8	Takeaways	54
4.9	Reflection	54

5	Install With Secure Defaults	55
5.1	In plain terms	55
5.1.1	Chapter contract	55
5.2	The decision at stake	55
5.3	Working model	56
5.3.1	See the chapter in practice	56
5.3.2	Chapter-specific operating protocol	58
5.3.3	Operating workflow	60
5.3.4	Evidence and control graph	61
5.4	Worked composite case file — illustrative, not empirical evidence	62
5.4.1	Scenario trace	63
5.4.2	Artifact handoff	64
5.4.3	Evidence application	64
5.4.4	Transfer test	64
5.5	Measurement and recovery decision	64
5.6	Practice lab	65
5.7	Limits and judgment	65
5.8	Takeaways	66
5.9	Reflection	66
6	Control the Document Pipeline	67
6.1	In plain terms	67
6.1.1	Chapter contract	67
6.2	The decision at stake	67
6.3	Working model	68
6.3.1	See the chapter in practice	68
6.3.2	Chapter-specific operating protocol	70
6.3.3	Operating workflow	72
6.3.4	Evidence and control graph	73
6.4	Worked composite case file — illustrative, not empirical evidence	74
6.4.1	Scenario trace	75
6.4.2	Artifact handoff	76
6.4.3	Evidence application	76
6.4.4	Transfer test	76
6.5	Measurement and recovery decision	76
6.6	Practice lab	77
6.7	Limits and judgment	77
6.8	Takeaways	78
6.9	Reflection	78
	Midpoint visual synthesis	79
7	Evaluate the Task, Not the Chat	81
7.1	In plain terms	81
7.1.1	Chapter contract	81
7.2	The decision at stake	81
7.3	Working model	82

7.3.1	See the chapter in practice	82
7.3.2	Chapter-specific operating protocol	84
7.3.3	Operating workflow	86
7.3.4	Evidence and control graph	87
7.4	Worked composite case file — illustrative, not empirical evidence	88
7.4.1	Scenario trace	89
7.4.2	Artifact handoff	90
7.4.3	Evidence application	90
7.4.4	Transfer test	90
7.5	Measurement and recovery decision	90
7.6	Practice lab	91
7.7	Limits and judgment	91
7.8	Takeaways	92
7.9	Reflection	92
8	Constrain Tools and Actions	93
8.1	In plain terms	93
8.1.1	Chapter contract	93
8.2	The decision at stake	93
8.3	Working model	94
8.3.1	See the chapter in practice	94
8.3.2	Chapter-specific operating protocol	96
8.3.3	Operating workflow	98
8.3.4	Evidence and control graph	99
8.4	Worked composite case file — illustrative, not empirical evidence	100
8.4.1	Scenario trace	101
8.4.2	Artifact handoff	102
8.4.3	Evidence application	102
8.4.4	Transfer test	102
8.5	Measurement and recovery decision	102
8.6	Practice lab	103
8.7	Limits and judgment	103
8.8	Takeaways	104
8.9	Reflection	104
9	Design Hybrid Routing	105
9.1	In plain terms	105
9.1.1	Chapter contract	105
9.2	The decision at stake	105
9.3	Working model	106
9.3.1	See the chapter in practice	106
9.3.2	Chapter-specific operating protocol	108
9.3.3	Operating workflow	110
9.3.4	Evidence and control graph	111
9.4	Worked composite case file — illustrative, not empirical evidence	112
9.4.1	Scenario trace	113

9.4.2	Artifact handoff	114
9.4.3	Evidence application	114
9.4.4	Transfer test	114
9.5	Measurement and recovery decision	114
9.6	Practice lab	115
9.7	Limits and judgment	115
9.8	Takeaways	116
9.9	Reflection	116
10	Operate Updates and Regressions	117
10.1	In plain terms	117
10.1.1	Chapter contract	117
10.2	The decision at stake	117
10.3	Working model	118
10.3.1	See the chapter in practice	118
10.3.2	Chapter-specific operating protocol	120
10.3.3	Operating workflow	122
10.3.4	Evidence and control graph	123
10.4	Worked composite case file — illustrative, not empirical evidence	124
10.4.1	Scenario trace	125
10.4.2	Artifact handoff	126
10.4.3	Evidence application	126
10.4.4	Transfer test	126
10.5	Measurement and recovery decision	126
10.6	Practice lab	127
10.7	Limits and judgment	127
10.8	Takeaways	128
10.9	Reflection	128
11	Back Up Without Recreating Exposure	129
11.1	In plain terms	129
11.1.1	Chapter contract	129
11.2	The decision at stake	129
11.3	Working model	130
11.3.1	See the chapter in practice	130
11.3.2	Chapter-specific operating protocol	132
11.3.3	Operating workflow	134
11.3.4	Evidence and control graph	135
11.4	Worked composite case file — illustrative, not empirical evidence	136
11.4.1	Scenario trace	137
11.4.2	Artifact handoff	138
11.4.3	Evidence application	138
11.4.4	Transfer test	138
11.5	Measurement and recovery decision	138
11.6	Practice lab	139
11.7	Limits and judgment	139

11.8	Takeaways	140
11.9	Reflection	140
12	Build the Operating Runbook	141
12.1	In plain terms	141
12.1.1	Chapter contract	141
12.2	The decision at stake	141
12.3	Working model	142
12.3.1	See the chapter in practice	142
12.3.2	Chapter-specific operating protocol	144
12.3.3	Operating workflow	146
12.3.4	Evidence and control graph	147
12.4	Worked composite case file — illustrative, not empirical evidence	148
12.4.1	Scenario trace	149
12.4.2	Artifact handoff	150
12.4.3	Evidence application	150
12.4.4	Transfer test	150
12.5	Measurement and recovery decision	150
12.6	Practice lab	151
12.7	Limits and judgment	151
12.8	Takeaways	152
12.9	Reflection	152
	Closing: keep the evidence visible	153
	A compact implementation workbook	155
	Decision register	156
	Evidence scorecard	157
	Exception log	158
	Ninety-day plan	159
	Control and test matrix	160
	Workflow map	161
13	References	163

Define the Boundary Before the Model

In plain terms

Locality is one control property, not the complete privacy objective. In a local-first knowledge and model stack, the practical question is **What data, systems, and people must the local design protect?** For technical professionals and privacy-conscious teams evaluating on-device or self-hosted language models, the answer counts only when **Draw data sources, process boundaries, network paths, users, storage, and deletion points** produces reviewable evidence for **unapproved boundary crossings** without normalizing **equating localhost with private**.

Chapter contract

DECIDE

What data, systems, and people must the local design protect?

BUILD

Draw data sources, process boundaries, network paths, users, storage, and deletion points.

MEASURE

unapproved boundary crossings

STOP OR REDESIGN WHEN

equating localhost with private

The decision at stake

For **Define the Boundary Before the Model**, the deployment owner must decide **what data, systems, and people must the local design protect?** before the sensitive task crosses from discussion into consequence for the data owner and authorized users. The minimum decision record is the artifact **Draw data sources, process boundaries, network paths, users, storage, and deletion points**, the observable **unapproved boundary crossings**, and the explicit hold condition **equating localhost with private**. If any Chapter 1 field is missing, the safe default is to disconnect external access and restore the last verified local path.

The bounded **Define the Boundary Before the Model** decision

advances the book's promise to design and operate a local AI workflow with explicit data boundaries, realistic hardware expectations, testing, and secure defaults. It does not endorse a product or predetermine the Chapter 1 answer; it creates a record that another person can challenge for every version change, benchmark, deletion test, and restore drill.

Working model

Read the **Define the Boundary Before the Model** model as four linked fields. **Outcome:** Locality is one control property, not the complete privacy objective. **Boundary:** the design must make **equating localhost with private** visible rather than convenient. **Evidence:** interpret **unapproved boundary crossings** together with review effort and excluded cases. **Authority:** the deployment owner may continue, narrow, escalate, or stop the sensitive task. For **Define the Boundary Before the Model**, Reference [4] from National Institute of Standards and Technology, *Privacy Framework*, informs a Chapter 1 boundary; it is not evidence that the local method or illustrative target will work.

See the chapter in practice

The **define the data boundary before the model in practice** maps *Local First, AI Second* Chapter 1 into a field scene before its abstract models begin. In one frame, it holds the question **What data, systems, and people must the local design protect?**, the artifact **Draw data sources, process boundaries, network paths, users, storage, and deletion points.**, the proof signal **unapproved boundary crossings**, and the warning **equating localhost with private**.

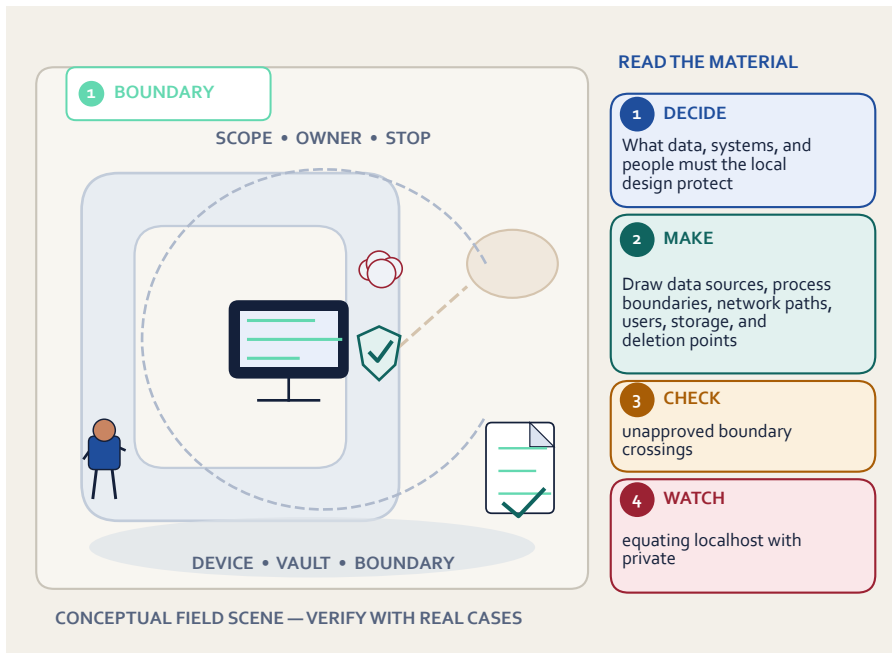


Figure 1.1: Chapter 1 field scene for Define the Boundary Before the Model: a boundary view in the book's local first setting.

Read the scene: For Local First, AI Second, Chapter 1, begin with the central local first scene and scan DECIDE, MAKE, CHECK, and WATCH. Treat the Define the Boundary Before the Model scene as conceptual, then use its cases and evidence records to test whether unapproved boundary crossings actually improves. For **Define the Boundary Before the Model**, this explanatory plate is a reasoning prompt—not observed evidence or a universal operating prescription.

Visual field note — Define the Boundary Before the Model:

- 1. Locate the tension.** In this composite situation, A consultancy separates client documents from public model experiments.
- 2. Name the choice.** Answer the chapter question: **What data, systems, and people must the local design protect?**
- 3. Produce the record.** Use **Draw data sources, process boundaries, network paths, users, storage, and deletion points.**, then retain the deployment owner, assumptions, and case evidence needed to review it.
- 4. Test and return.** Track **unapproved boundary crossings**. If **equating localhost with private**, return to DECIDE and revise the data boundary instead of explaining the warning away.

Chapter-specific operating protocol

Phase	Reader action	Evidence retained	Hold condition
1. Define	Write the exact decision behind What data, systems, and people must the local design protect? .	Chapter 1 owner, input, output, exception, and timestamp.	Hold Define the Boundary Before the Model if its record cannot be reconstructed.
2. Contrast	Apply Draw data sources, process boundaries, network paths, users, storage, and deletion points to one ordinary case.	Chapter 1 owner, input, output, exception, and timestamp.	Hold Define the Boundary Before the Model if its record cannot be reconstructed.
3. Exclude	Run the same artifact against a counter case shaped by equating localhost with private .	Chapter 1 owner, input, output, exception, and timestamp.	Hold Define the Boundary Before the Model if its record cannot be reconstructed.
4. Assign	Name the deployment owner as the person who may continue, narrow, or stop.	Chapter 1 owner, input, output, exception, and timestamp.	Hold Define the Boundary Before the Model if its record cannot be reconstructed.
5. Challenge	Record unapproved boundary crossings and the review effort for the same case.	Chapter 1 owner, input, output, exception, and timestamp.	Hold Define the Boundary Before the Model if its record cannot be reconstructed.

Phase	Reader action	Evidence retained	Hold condition
6. Publish	Release the Define the Boundary Before the Model artifact only when its evidence answers this chapter's question.	Chapter 1 owner, input, output, exception, and timestamp.	Hold Define the Boundary Before the Model if its record cannot be reconstructed.

This sequence is specific to **Define the Boundary Before the Model**. For that Chapter 1 decision, it is not permission to automate; it is a way for technical professionals and privacy-conscious teams evaluating on-device or self-hosted language models to make the reasoning inspectable for every version change, benchmark, deletion test, and restore drill.

Draw data sources, process boundaries, network paths, users, storage, and deletion points. This is the chapter's core production artifact. The **Define the Boundary Before the Model** artifact should fit on one page, use ordinary language, and be reviewed by someone who did not design it. A compact artifact exposes disagreements that a long narrative can conceal.

The chapter's visual tool is the **chapter contract**. For **Define the Boundary Before the Model**, it translates explanation into an inspectable decision aid: the reader can see the decision, artifact, evidence, and exact condition that pauses the sensitive task.

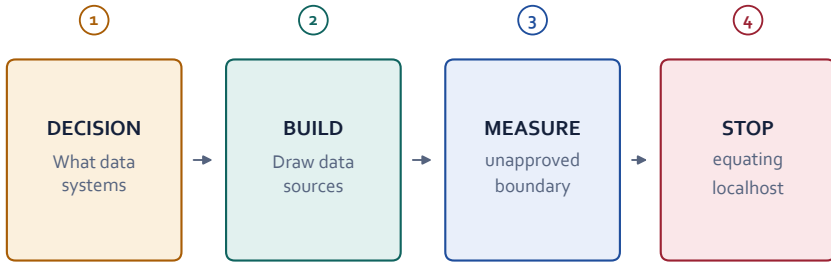


Figure 1.2: Chapter contract connecting the decision, artifact, measure, and stop condition for Define the Boundary Before the Model.

How to use this page: Move across the four Define the Boundary Before the Model cards; compare the decision with unapproved boundary crossings and stop before equating localhost with private. The chapter-specific measure is **unapproved boundary crossings**; the principal warning is **equating localhost with private**.

Operating workflow

The **define the data boundary before the model workflow** makes the chapter executable. For **Define the Boundary Before the Model**, the five stages carry **Draw data sources, process boundaries, network paths, users, storage, and deletion points.** from the question **What data, systems, and people must the local design protect?** to a test against **unapproved boundary crossings**, with **equating localhost with private** as an explicit return or stop signal.

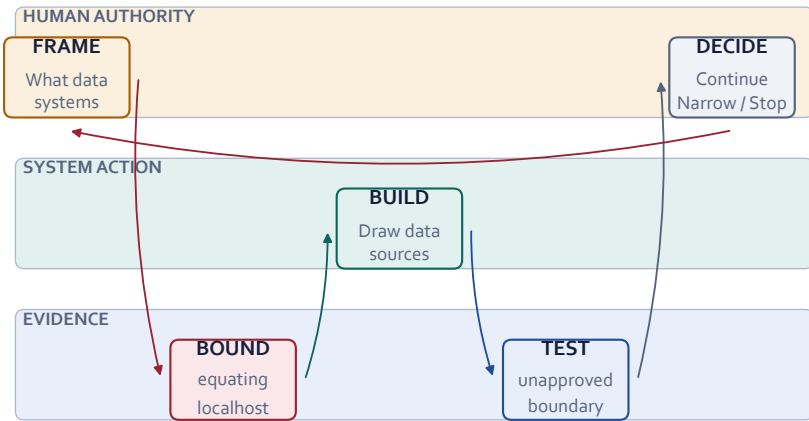


Figure 1.3: Five-stage workflow for chapter 1, Define the Boundary Before the Model: frame the decision, set the data boundary, build Draw data sources, process boundaries, network paths, users, storage, and deletion points., test against unapproved boundary crossings, then continue, narrow, or stop before equating localhost with private.

Read the workflow: Move from FRAME to DECIDE for Define the Boundary Before the Model. The lower return path is mandatory when evidence is missing or the stop signal—equating localhost with private—appears. For **Define the Boundary Before the Model**, record the deployment owner and evidence at every handoff; an arrow is not evidence that the preceding stage passed.

Evidence and control graph

The **define the data boundary before the model — evidence network** shows the relationships that must remain inspectable when the workflow runs. In *Local First, AI Second*, this qualitative graph asks the reader to record observed evidence for **unapproved boundary crossings** and route **equating localhost with private** to recovery instead of treating sample numbers as facts.

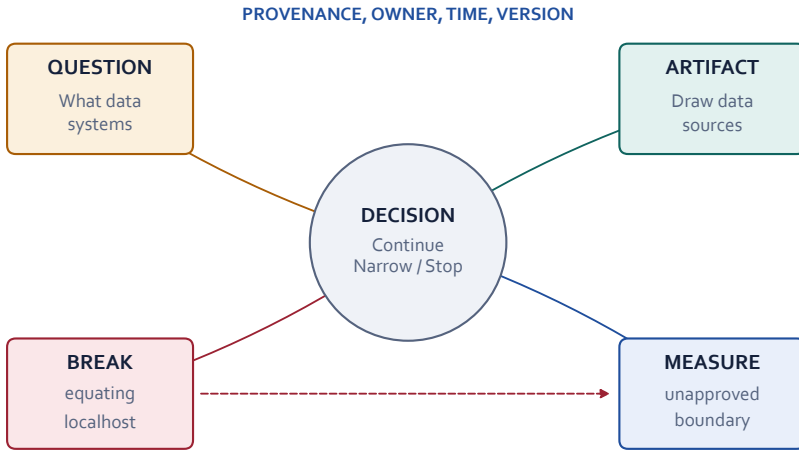


Figure 1.4: Qualitative evidence network for chapter 1, Define the Boundary Before the Model, linking the question to Draw data sources, process boundaries, network paths, users, storage, and deletion points., the measure unapproved boundary crossings, and the recovery condition equating localhost with private without invented empirical values.

Read the graph: Trace the evidence for Define the Boundary Before the Model toward the decision. For Define the Boundary Before the Model, empty or weak evidence does not count as zero risk; it routes the sensitive task to verification, escalation, or stop. Use this **Define the Boundary Before the Model** graph beside **Draw data sources, process boundaries, network paths, users, storage, and deletion points**, not as a substitute for recorded cases.

Worked composite case file — illustrative, not empirical evidence

This **Define the Boundary Before the Model** record turns the scenario into an inspectable rehearsal in a local-first knowledge and model stack. Its numbers are worksheet examples for Chapter 1, not observed results or a prediction of benefit.

Record field	Filled illustrative entry
Situation	A consultancy separates client documents from public model experiments.
People affected	the data owner and authorized users
Decision	What data, systems, and people must the local design protect?
Artifact excerpt	Draw data sources, process boundaries, network paths, users, storage, and deletion points.
Accountable authority	The deployment owner.
Measure and unit	unapproved boundary crossings — one dated observation for each eligible case.
Example baseline	7 observations in the baseline window.
Example target / decision rule	a documented improvement plus no severe unresolved exception; move only contextual; the deployment owner must define better before collection.
Named exception	equating localhost with private.
Safe default	Disconnect external access and restore the last verified local path.

Scenario trace

1. **Preserve the starting state.** For **Define the Boundary Before the Model**, record the original request, governing rule, available evidence, and the last safe result before changing anything.
2. **Make the chapter decision.** Answer **What data, systems, and people must the local design protect?** and record the Chapter 1 assumption that carries the most consequence for the data owner and authorized users.
3. **Use the artifact.** Complete **Draw data sources, process boundaries, network paths, users, storage, and deletion points** with a normal case and a counter case; in this chapter, do not infer missing facts merely to finish the form.
4. **Observe the decision rule.** Review **unapproved boundary crossings** for every version change, benchmark, deletion test, and restore drill; the **Define the Boundary Before the Model** record reports exclusions and review effort beside the headline value.

5. **Contain and recover.** If **equating localhost with private**, disconnect external access and restore the last verified local path. Preserve the Chapter 1 failed case, assign a deadline, and require the deployment owner to authorize any restart.

Artifact handoff

Start **Define the Boundary Before the Model** from the book-level thesis and boundary. Within *Local First, AI Second*, attach the current artifact and exception record, then hand both to Chapter 2, **Classify the Workload**, which asks: Which tasks justify local inference and which do not?. That recipient may revise the **Define the Boundary Before the Model** assumption, but must preserve the evidence that made this book's earlier decision reasonable.

Evidence application

Reference [4], National Institute of Standards and Technology, *Privacy Framework*, provides a relevant boundary or design input for **Define the Boundary Before the Model**. It does **not** prove that the Chapter 1 worked values, local method, or target will succeed. The **Define the Boundary Before the Model** reviewer must link this book's exact claim to the exact source passage and leave unsupported synthesis marked UNVERIFIED.

Transfer test

- Re-run **Draw data sources, process boundaries, network paths, users, storage, and deletion points** with one routine Chapter 1 case that should pass.
- Re-run the **Define the Boundary Before the Model** artifact with missing evidence and keep the safe default active.
- Re-run it where **equating localhost with private** appears plausible but not certain.
- Ask a reviewer who did not design this chapter's method to decide whether the retained record supports continuing, narrowing, escalating, or stopping.

Measurement and recovery decision

For **Define the Boundary Before the Model**, define **unapproved boundary crossings** as one dated observation for each eligible case. In this **Define the Boundary Before the Model** worksheet, the Chapter 1 worked baseline is 7 observations in the baseline window and the illustrative target is a documented improvement plus no severe unresolved exception; both must be replaced with evidence from a local-first knowledge and model

stack. Review the Chapter 1 result for every version change, benchmark, deletion test, and restore drill, preserve excluded and high-consequence cases, and interpret movement as better only when it is contextual; the deployment owner must define better before collection.

The named failure is **equating localhost with private**. Containment means: disconnect external access and restore the last verified local path. Recovery is complete only after the deployment owner can reconstruct the failed case, explain which assumption changed, and authorize a new test against **unapproved boundary crossings**.

Practice lab

Choose one live but reversible **Define the Boundary Before the Model** example from a local-first knowledge and model stack. Create the following:

- a one-sentence answer to **What data, systems, and people must the local design protect?**;
- a completed first draft of **Draw data sources, process boundaries, network paths, users, storage, and deletion points**;
- one routine case, one missing-evidence case, and one case shaped by **equating localhost with private**;
- a locally measured baseline for **unapproved boundary crossings** using the unit one dated observation for each eligible case;
- a stop threshold, the deployment owner as owner, and the safe default disconnect external access and restore the last verified local path;
- deployment evidence packet that will be handed to the next chapter.

Ask a colleague to challenge **Draw data sources, process boundaries, network paths, users, storage, and deletion points**. They should identify one ambiguous field, one person among the data owner and authorized users whose interests are missing, and one reason **unapproved boundary crossings** could reward the wrong behavior. Preserve that challenge in the chapter handoff before revising.

Limits and judgment

Define the Boundary Before the Model supplies a locally testable method, not proof of causal effectiveness or a universal rule. This Chapter 1 method remains inside the book boundary: This book is not a guarantee of privacy or security, does not endorse a model, and requires local legal, security, and hardware review for consequential use. Readers applying **Define the Boundary Before the Model** for the data owner and authorized users must verify current law, contract, policy, safeguarding, accessibility, security, and professional duties before consequential use. A

negative **unapproved boundary crossings** result may mean the question was framed badly, the review cost is too high, or disconnect external access and restore the last verified local path is the responsible decision.

Takeaways

- Locality is one control property, not the complete privacy objective.
- The chapter artifact is: draw data sources, process boundaries, network paths, users, storage, and deletion points.
- The primary measure is **unapproved boundary crossings**, paired with review cost and failure severity.
- Watch especially for **equating localhost with private**.
- In a local-first knowledge and model stack, expand scope only after the deployment owner can show the evidence and exercise the recovery path.

Reflection

What evidence would let a skeptical reviewer answer **What data, systems, and people must the local design protect?** differently from the deployment owner? Which case involving the data owner and authorized users would **unapproved boundary crossings** miss, and would that omission require continuing, narrowing, escalating, or disconnect external access and restore the last verified local path?