

COMPANION WORKSHEET

Chapter 1 — Ownership Decision

This is the only required worksheet for Chapter 1. Complete it for one real task. Short answers are enough; an honest Unknown is more useful than a confident guess.

Use the detailed companion tools only when a row below needs more work: DATA_FLOW_DIAGRAM.md traces a complicated request.

DATA_CLASSIFICATION_WORKSHEET.md separates data with different consequences.

THREAT_MODEL_CHECKLIST.md helps choose three plausible failures.

OWNERSHIP_MATRIX.md records several components or dependencies.

1. Define the task

Decision field	Your answer
Specific task	
People whose information or interests are involved	
Required capability	
Must it work without outside internet access?	Yes / No / Unknown
Must it work with every network interface disabled?	Yes / No / Unknown
Must it work without a vendor account?	Yes / No / Unknown
Is remote access required?	Yes / No / Unknown

2. Classify the complete request

Choose Unknown / unclassified, Routine, Personal, Sensitive, or Restricted.

The complete request includes the visible prompt, attached files, relevant history, retrieved passages, tool inputs and outputs, and the likely response.

Classification field	Your answer
Information class	
Most serious consequence if exposed, changed, lost, or retained unexpectedly	
Material to remove, redact, or keep out	
Retention expectation	

Restricted secrets such as passwords, recovery codes, authentication tokens, private keys, and full payment credentials do not belong in a general AI workflow.

3. Trace the important path

You do not need a perfect architecture diagram. Name the material components and mark unknowns.

Component or path	Where it operates	What it receives or stores	Evidence or unknown
Client or interface			
Model and runtime			
Documents, retrieval, or tools			
History, logs, and temporary state			
Accounts or outside services			
Backups or exports			

4. Apply the ownership test

Use only these four statuses:

Known and controlled

Known external dependency

Unknown

Not applicable

Ownership question	Status	Evidence or next check
Can I identify the material components and dependencies?		
Can I decide when the workflow operates and connects?		
Can I verify where important data goes and remains?		
Can I preserve or export the useful state?		
Can I restore or replace what matters?		

Do not convert Unknown into safe. Give each material unknown a disposition: investigate before use, reduce the information, accept temporarily with a review date, or choose another boundary.

5. Choose a provisional boundary

Boundary	Selected?	Why it fits or does not fit	Evidence still needed
Provider-operated service			

Boundary	Selected?	Why it fits or does not fit	Evidence still needed
Local client with remote processing			
Household-hosted service			
Single-device local workflow			
Deliberately disconnected workflow			
Split or hybrid boundary			

Compare the candidates against the task's consequences, required capability, outside dependencies, maintenance burden, recovery path, cost, and the strength of available evidence.

6. Name three plausible failures

Scenario	Proportionate control	Proof after the change
1.		
2.		
3.		

Prefer ordinary failures first: shared access, unintended network reachability, account loss, device theft, unsafe files, unintended retention, failed storage, or an unproved restore.

7. Record the decision

Final field	Your answer
Chosen boundary	
Accepted outside dependencies	
Material unknowns and their disposition	
Unique state that must survive	
Export, backup, restore, or replacement expectation	
Decision	Proceed / Proceed after changes / Use another boundary / Do not submit

Chapter stop point

Chapter 1 is complete when you can explain:

1. what you control; 2. what you knowingly depend on; 3. what remains unknown; 4. why the chosen boundary fits this task; and 5. what later chapters must prove before you trust it.

Do not solve every unknown now. Carry the record forward and resolve each item in the chapter that owns the test.