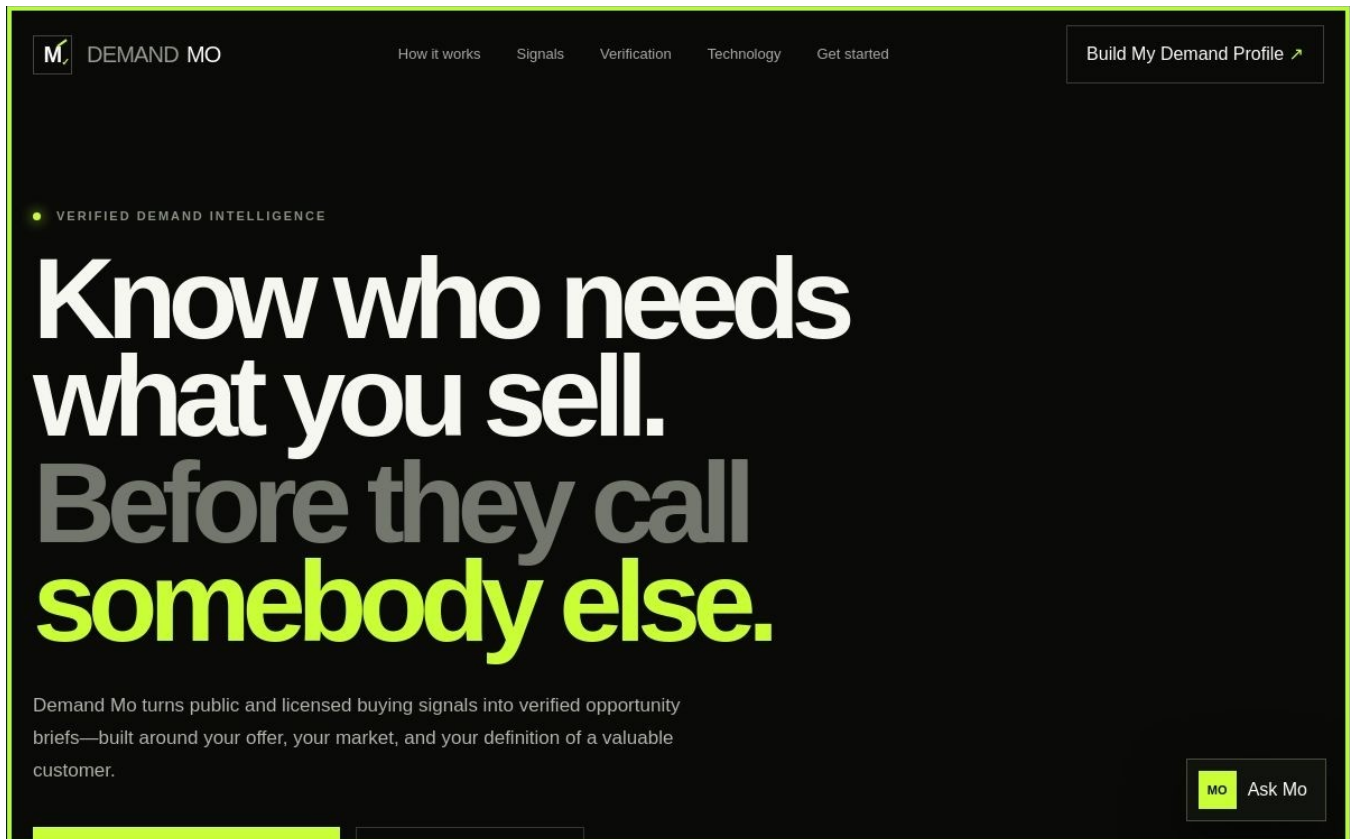


Customer Onboarding System (COS)

A repeatable operating system for activating new Demand Mo users and teams.



Production guide • Version 1.0 • 17 August 2026

Purpose and graduation standard

The COS moves a user from orientation to a repeatable weekly demand-intelligence workflow. A user graduates when they can create a Demand Profile, interpret evidence, use Ask Mo, explain why an opportunity matters now, and document a responsible next action.

Audience	Primary job	Graduation evidence
New user	Find and understand qualified demand	Saved profile + one evidence-led opportunity brief
Sales / BD	Prioritize outreach	A researched account and defensible next step
Manager	Set standards and coach usage	Quality review and weekly operating cadence
Administrator	Control access, policy, and integrations	Approved sources, roles, retention, and command scope

Learning outcomes

- Describe what Demand Mo does—and what it does not do.
- Build a Demand Profile using offer, market, buyer, geography, and signal criteria.
- Separate raw signals from verified evidence and clearly label uncertainty.
- Use Ask Mo for product guidance without assuming it is a general-purpose autonomous agent.
- Apply the seven-question Opportunity Reasoning Engine consistently.
- Operate within privacy, licensing, source-terms, and human-approval requirements.

Onboarding journey

Stage	Timing	Owner	Activity	Pass condition
0. Prepare	Before Day 1	Admin	Approve audience, data sources, roles, command permissions	Workspace and policy ready
1. Orient	Day 1 · 15 min	Champion	Tour value proposition, navigation, Ask Mo	User can locate every primary control
2. Profile	Day 1 · 20 min	User	Create first Demand Profile	Reference ID recorded
3. Evidence	Day 2 · 30 min	Coach	Review source, recency, corroboration, confidence	User explains evidence chain
4. Reason	Day 2 · 30 min	User	Answer seven opportunity questions	Brief is complete and traceable
5. Act	Day 3	User + manager	Choose a	Action and owner

			proportionate human-approved next step	assigned
6. Embed	Days 4–7	Manager	Run first weekly review	Cadence, metrics, and escalation path agreed

Module 1 — Product orientation

Outcome: distinguish a verified opportunity brief from a lead list. Exercise: explain the homepage promise in your own words and identify the profile and guide controls.

Module 2 — Demand Profile

Outcome: define a narrow, testable search thesis. Exercise: enter one offer, buyer problem, market, geography, signal type, and exclusion; submit and retain the DM reference.

Module 3 — Signals and verification

Outcome: assess evidence quality. Use a four-part check: source legitimacy, direct relevance, recency, and independent corroboration.

Module 4 — Ask Mo

Outcome: obtain product help. Ask one navigation question, one profile question, and one verification question; confirm that responses describe a next step rather than silently executing external actions.

Module 5 — Opportunity reasoning

Outcome: produce a brief answering: company; problem; evidence; cost; decision owner; solution; why now.

Module 6 — Responsible action

Outcome: choose outreach or investigation proportional to confidence. Never infer sensitive traits, bypass access controls, or contact people automatically without approved policy.

Module 7 — Team operating rhythm

Outcome: run a weekly 30-minute review: new profiles, evidence quality, qualified briefs, next actions, false positives, source issues, and feedback.

Facilitator runbook

Minute	Facilitator action	Participant action
0–5	Set outcome and boundaries	State use case
5–15	Demonstrate navigation	Follow along
15–30	Coach profile creation	Submit profile
30–45	Teach evidence rubric	Score an example
45–60	Guide seven-question brief	Complete brief
60–70	Review Ask Mo	Ask two questions
70–80	Agree next action and cadence	Commit owner/date

Quality rubric

Dimension	Ready	Needs work
Profile	Specific offer, problem, market, and signals	Broad market or missing exclusions
Evidence	Traceable, current, corroborated	Single weak or ambiguous signal
Reasoning	All seven questions answered	Claims outrun evidence
Action	Named owner, date, human approval	Automated or undefined outreach
Governance	Approved sources and retention	Unknown license, terms, or privacy basis

30-day success measures

- Activation: profile submitted and Ask Mo used during first session.
- Time to first qualified brief.
- Percentage of briefs with traceable evidence and all seven questions complete.
- False-positive rate and reasons.
- Weekly active users and completed review cadence.
- Zero unauthorized source, privacy, or remote-command incidents.

Administrator production checklist

- Confirm public pages contain no demo claims, fabricated customers, or fake live metrics.
- Audit every repository, dependency, model, data source, and deployment artifact for license and source terms.
- Restrict SSS Brain remote commands to an authenticated allowlist; log requester, command, result, and timestamp; require human approval for consequential actions.
- Configure secrets outside source control; rotate keys; apply least privilege; test backup and recovery.
- Set privacy notice, retention, deletion, incident response, accessibility, monitoring, and support ownership.
- Run acceptance tests for profile submission, Ask Mo, mobile layout, keyboard use, download links, API health, and failure states.

Open-source implementation map

Capability	Preferred V1	Controlled / optional
Crawling	Crawl4AI, Scrapy	Playwright when rendering is required
Recon	SpiderFoot, HTTPX	WAFW00F with authorization
Browser assistance	Playwright	Nanobrowser after security review
Local AI	Ollama	Model license and hardware review

Identity discovery	—	Maigret / Sherlock only for lawful approved use
Storage	PostgreSQL + pgvector	Qdrant if operational need justifies it

Repository licenses above are top-level indicators, not legal clearance. Complete dependency, model, content, privacy, and terms-of-service reviews before production use.

Support and escalation

Product question → Ask Mo. Data or evidence concern → team reviewer. Access or integration concern → administrator. Suspected privacy/security incident → stop the workflow, preserve logs, and follow the organization's incident-response process.