

DIFC wealth AI, *tick by tick*

Every task from an empty office cabinet to the day the compliance officer signs go-live. Nine modules, one matrix for the twelve workflows, a signature line under each module. Tick it here, or download the PDF and work through it on paper.

1. FOUNDATIONS
Office, server, data

2. GOVERN
DIFC + DFSA, build tool

3. BUILD
The loop + 12 workflows

4. GO LIVE
Training + sign-off

01 OFFICE AND HARDWARE

PHASE 1 • FOUNDATIONS

0 / 8

☐ World 1 machines listed: AI server, adviser PCs, compliance PC

☐ World 2 internet desk placed apart, orange label on its screen

☐ Server chosen: Mac Studio 192 GB+ or 1 to 2 GPU server

☐ Locked cabinet, UPS (15 min) and managed switch installed

☐ Two 4 TB encrypted backup drives (A and B) and a small safe bought

☐ Router serves only World 2 and guest Wi-Fi, no port into the World 1 switch

☐ Encrypted transfer drive bought, logbook started for every trip in and out

☐ Every World 1 PC and laptop has full-disk encryption on

Owner

Date done

Checked by

02

SERVER BUILD AND LOCKDOWN

PHASE 1 · FOUNDATIONS

0 / 11

- | | | |
|--------------------------|---|--------------------|
| ☐ | Ubuntu Server 24.04 LTS installed with LUKS full-disk encryption | step 1 |
| ☐ | Roles created: advisers, compliance, ops | 01-setup-server.sh |
| ☐ | Folder tree /srv/wealth created with correct owners | 01-setup-server.sh |
| ☐ | Idle lock (15 min) and auditd watch on client folders running | 01-setup-server.sh |
| ☐ | Firewall denies all outgoing, LAN only allowed in | 02-firewall.sh |
| ☐ | DOCKER-USER chain drops container traffic leaving the LAN | 02-firewall.sh |
| ☐ | Proof test prints OK: no internet, screenshot filed for compliance | 02-firewall.sh |
| ☐ | WAN cable removed from the server for good | |
| ☐ | Model and images carried in on the transfer drive, docker load done | step 3 |
| ☐ | docker compose up -d: ollama, db, app, chat, caddy all healthy | docker-compose.yml |
| ☐ | HTTPS root certificate installed on every office PC | Caddyfile |

Owner

Date done

Checked by

03

DATA, ACCESS AND BACKUPS

PHASE 1 · FOUNDATIONS

0 / 10

- | | | |
|--------------------------|---|-----------------|
| ☐ | Database schema loaded, ai_audit_log refuses edits and deletes (tested) | schema.sql |
| ☐ | Every staff member added to the staff table with the right role | schema.sql |
| ☐ | Staff logins created in Caddy, no shared logins | Caddyfile |
| ☐ | Client folders opened by script only, client IDs never names | new-client.sh |
| ☐ | Adviser test: adviser A cannot see adviser B's client | app/main.py |
| ☐ | Compliance test: compliance sees every client | app/main.py |
| ☐ | Nightly backup at 22:00 in cron, first run checked in backup.log | backup.sh |
| ☐ | Restic password sealed on paper in the safe | |
| ☐ | First restore test done on a sample client and logged | restore-test.sh |
| ☐ | Retention set: 72 monthly snapshots, retain_until per client | backup.sh |

Owner

Date done

Checked by

04

DIFC AND DFSA GOVERNANCE

PHASE 2 • GOVERN

0 / 9

- | | | |
|--------------------------|---|-----------------|
| ☐ | AI-use policy written and approved by partners | Document 1 |
| ☐ | AI register started, one line per workflow key | Document 2 |
| ☐ | Impact assessment done for onboarding and KYC first | Document 3 |
| ☐ | Client agreement names the AI system and what it does | DIFC DP Reg. 10 |
| ☐ | Decision recorded on Autonomous Systems Officer and Commissioner approval | DIFC DP Reg. 10 |
| ☐ | Outsourcing agreement, NDA, risk assessment and exit plan signed | DFSA GEN 5.3 |
| ☐ | Breach steps written: who calls the DIFC Commissioner and when | DIFC DPL 2020 |
| ☐ | Record keeping: six years confirmed, retrieval tested | DFSA GEN |
| ☐ | Compliance officer checked every rules line against the current rulebook | |

Owner

Date done

Checked by

05

BUILD MACHINE AND CLAUDE CODE

PHASE 2 • GOVERN

0 / 7

- | | | |
|--------------------------|---|-----------------------|
| ☐ | Build machine kept on World 2 with sample clients only (C-9001 to C-9099) | CLAUDE.md |
| ☐ | managed-settings.json installed in /etc/claude-code/, owned by root | managed-settings.json |
| ☐ | Deny list active: WebFetch, WebSearch, curl, wget, scp, ssh, client folders | managed-settings.json |
| ☐ | Bypass permissions mode disabled | managed-settings.json |
| ☐ | Audit hook logs every tool call to claude-code.log | audit-hook.sh |
| ☐ | Hook block tested: a call naming /srv/wealth/clients is refused | audit-hook.sh |
| ☐ | CLAUDE.md firm rules reviewed by compliance | CLAUDE.md |

Owner

Date done

Checked by

- | | | |
|--------------------------|--|--------------------|
| ☐ | House rules in jobs.py: drafts only, never a product, MISSING not guesses, [p.N] on every figure | jobs.py |
| ☐ | PDF upload adds page markers so drafts can cite [p.N] | app/main.py |
| ☐ | Model runs at temperature 0.1 | app/main.py |
| ☐ | Every draft waits in the review queue, nothing files itself | app/main.py |
| ☐ | Approve writes to the client folder with the approver's name in the file name | app/main.py |
| ☐ | Reject returns the draft with a reason | |
| ☐ | Every draft, view, approve and reject hashed into ai_audit_log | app/main.py |
| ☐ | Check: nobody approved a job they created (query 3 returns no rows) | monthly-sample.sql |

Owner

Date done

Checked by

#	JOB	AI DOES	HUMAN DOES	WORLD	PROMPT IN JOBS.PY	TESTED ON 3 FILES	ON AI REGISTER	LIVE, OWNER NAMED
1	Prospect brief	Public sources, service match, first email	Checks every fact link	2	☐	☐	☐	☐
2	Onboarding pipeline	Stage per client, chases missing items	Compliance signs file	1	☐	☐	☐	☐
3	Fact-find and KYC	Reads documents, fills fields, flags MISSING	Confirms every field	1	☐	☐	☐	☐
4	Meeting prep and note	Brief before, file note after	Adviser reviews	1	☐	☐	☐	☐
5	Suitability report	First draft from fact-find and model	Adviser edits, signs	1	☐	☐	☐	☐
6	Portfolio drift	Daily check vs model, flags tolerance	Decides rebalance	1	☐	☐	☐	☐
7	Equity and bond screen	House rules, reason per pass or fail	Analyst signs shortlist	1	☐	☐	☐	☐
8	Research notes	40 pages to 1, page numbers on figures	Clicks references	1	☐	☐	☐	☐
9	News watch	Matches news to client segments	Reads primary source	2	☐	☐	☐	☐
10	Client update emails	Personal draft from own numbers	Approves, sends from mail desk	1	☐	☐	☐	☐
11	Staff follow-ups	Actions become tasks with owner and date	Manager reviews weekly	1	☐	☐	☐	☐
12	Audit log and verify	Logs prompt, output, approver, source	Compliance samples monthly	1	☐	☐	☐	☐

Owner

Date done

Checked by

08

TRAINING

PHASE 4 • GO LIVE

0 / 8

- ☐ Partners and leadership, 90 minutes: policy and register approved
- ☐ Advisers and para-planners, half day: each ran one job on a sample client
- ☐ Advisers found the planted wrong figure in a draft
- ☐ Compliance officer, half day: ran the three monthly audit queries `monthly-sample.sql`
- ☐ IT and ops, full day: rebuilt steps 1 to 9 from the kit
- ☐ IT and ops: drive swap and restore test done hands-on `restore-test.sh`
- ☐ Every user signed the AI-use policy
- ☐ Always / Never sheet pinned at every World 1 desk `guide #guide`

Owner

Date done

Checked by

09

GO-LIVE SIGN-OFF

PHASE 4 • GO LIVE

0 / 10

- ☐ Pilot ran 2 weeks beside the old way, hours logged daily
- ☐ Go or no-go decided on the firm's own numbers
- ☐ First monthly audit-log sample by compliance done
- ☐ Backup log shows 7 nights in a row, drives swapped on Monday
- ☐ Quarterly restore test booked in the calendar
- ☐ Every login and password handed back to the firm
- ☐ Runbook and recorded walkthrough delivered
- ☐ Incident table (first 10 minutes) printed for ops and compliance
- ☐ Next model and patch update date set (transfer drive)
- ☐ Compliance officer signs go-live

Owner

Date done

Checked by

Before sign-off: the rules column summarises the DIFC Data Protection Law No. 5 of 2020, Regulation 10, and DFSA GEN 5.3. The firm's compliance officer checks each line against the current rulebook. Code references point to the server kit at azizsaif.com/DIFC-ai-wealth-management/difc-wealth-kit.zip.