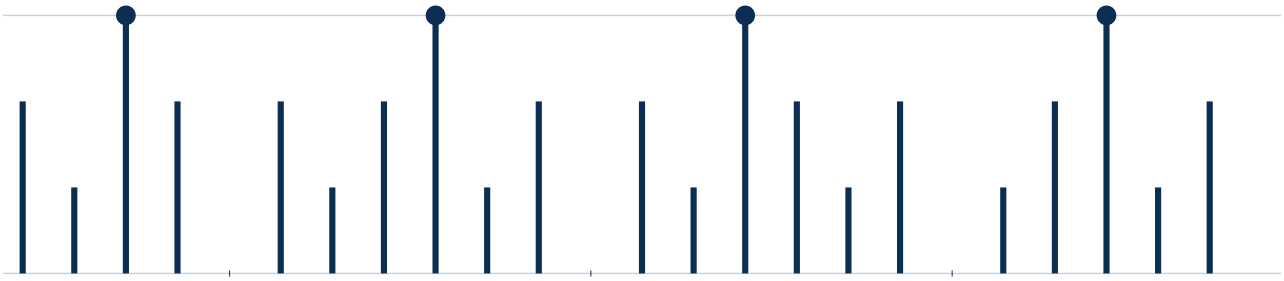
SERVICE TOUR

# Inside a digital asset risk assessment

A tour of the assessment application on a fictitious licensed firm, from the first interview to the reports the client receives.



| DATE | AUDIENCE | FORMAT | VERSION |
|---|---|---|---|
| 28 September 2026 | Principals, family offices and licensed firms | Illustrated walkthrough | 1.0 |

Olivier Busolini

© Olivier BUSOLINI - 2026 - No reuse without permission

# Contents

*This document walks through one complete assessment in the application that runs a digital asset risk engagement. The client is fictitious: Meridian Gulf Family Office, a VARA-licensed multi-family office in Dubai serving twelve client families, prepared as test data so that every screen carries realistic content without describing a real firm. The tour follows the order of the work. It opens with the engagement, where the client's type, regulatory standing and size set the bar the assessment measures against, then covers the interviews, the answers drafted from a transcript and the control assessment. It shows what the assessment finds and what it recommends, in what order, and what the client receives: a report kept as issued, a notice for findings that cannot wait, and a reassessment that shows what moved. The last section shows how the client's material is handled: what is sent to the AI assistant and what never is, and a chained record of every action. Nineteen screens illustrate the tour; Appendix A lists them and Appendix B records how the assessment behind them was prepared.*


| | | |
|---|---|---|
| 01 | The engagement, and the bar it is measured against<br>What the client is, what it does and who regulates it, before a single question is asked. | 4 |
| 02 | Interviews, drafted answers and the control assessment<br>Structured interviews, one session at a time, with every answer traceable to what was said. | 7 |
| 03 | What the assessment finds<br>One register for the engagement, scored from the answers, with the urgent findings raised first. | 12 |
| 04 | What to do, and in what order<br>Priority and urgency are derived from the rules; the consultant's judgement is recorded, not hidden. | 15 |
| 05 | What the client receives<br>A report that is refused until the assessment is complete, kept as issued, and compared next time. | 18 |
| 06 | How the client's material is handled<br>What leaves the consultant's machine, what never does, and what is recorded. | 20 |
| 07 | Sources<br>The documents and pages this one draws on. | 22 |
| A | Appendix A: the screens in this tour<br>Every figure, with the page it was taken from. | 23 |
| B | Appendix B: how this tour was prepared<br>The fictitious client, the transcript, and how the screens were captured. | 23 |


© Olivier BUSOLINI - 2026 - No reuse without permission

# Executive summary

- **What the client is and what it does both change the assessment.** Meridian is recorded as a licensed firm regulated by VARA alone, at tier T3 on operating profile F2, and those facts together set a maturity target of level 3 on every risk in scope.
- **Nineteen of the twenty-two modules apply, and the other three are gated off with a reason.** Collateral wallet services, sponsored VASPs and adjacent digital assets are out because the triage answers say the firm does none of them, which removes thirteen questions from the fieldwork.
- **Nothing is scored from a transcript until the consultant accepts it.** Each drafted answer quotes the interview word for word, and the application refuses a draft whose quotes are not in the transcript.
- **A question the interview did not reach stays open, and is not filled in.** Of twelve drafts from one session, eleven were accepted and one was left open for the follow-up.
- **The score is arithmetic, and the arithmetic is on the screen.** Likelihood times impact times an irreversibility multiplier, less a reduction for the protection in place, with each risk taking the lowest maturity among the controls mapped to it.
- **Sixty-eight risks were scored: four Critical, twenty High, twenty-nine Medium and fifteen Low.** The highest is blind signing, at 28.0, where approvers cannot verify what they are authorising.
- **Three findings are raised with the client before the report.** Blind signing, a departed analyst who still holds administrator access, and reconciliation breaks open since July.
- **Every recommendation is reviewed by the consultant, and the review is recorded.** Of fifty-five calculated, fifty-one were accepted, three edited and one rejected; twenty carried wording drafted by the AI assistant.
- **The roadmap is where prioritisation becomes a plan.** Forty-three actions fall in the first thirty days and eleven in the next thirty; the nine marked U1 start within seven days.
- **A final report is refused until every check passes.** Every recommendation reviewed, no out-of-date drafts, at least one accepted; the report is then filed with a fingerprint and the data behind it, and never overwritten.
- **A later assessment shows what moved.** Against report 1.0 the test client shows six risks improved, none slipped, four controls rated higher and three recommendations met.
- **The client is not named in the request that drafts the recommendations.** The client name, the consultant's name and the names of everyone interviewed are stripped out; the audit log chains each entry to the one before, and says plainly that it is a check and not a lock.

© Olivier BUSOLINI - 2026 - No reuse without permission

# 1

# The engagement, and the bar it is measured against

What the client is, what it does and who regulates it, before a single question is asked.

A licensed client's obligations raise the priority of a gap; an unregulated client's do not.

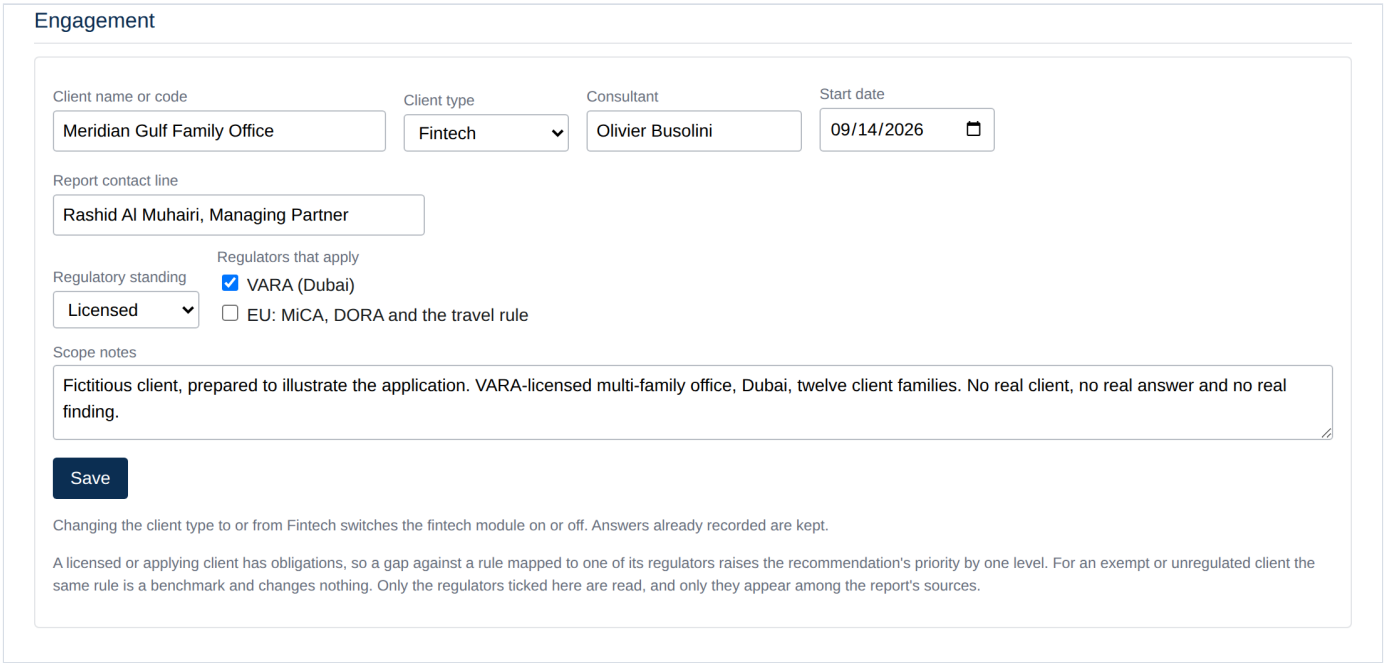
The tier and the operating profile together set the maturity target, at the higher of the two.

Triage decides what is asked at all: three modules out, thirteen questions removed.

An assessment starts by recording what the client is, because the same weakness carries a different weight for a private holder and for a firm holding other people's assets under a licence. The Overview page takes the client type, the regulatory standing and the regulators that apply. Meridian is recorded as *Fintech*, standing *Licensed*, with *VARA (Dubai)* ticked and the European instruments left unticked (Figure 1).

Those two fields do real work. The page states the rule where the consultant sets it: *"A licensed or applying client has obligations, so a gap against a rule mapped to one of its regulators raises the recommendation's priority by one level. For an exempt or unregulated client the same rule is a benchmark and changes nothing. Only the regulators ticked here are read, and only they appear among the report's sources"* (Overview page, DRA app 1.4.0). For Meridian that means the VARA rulebooks raise priorities and appear in the report; MiCA and DORA do neither.

**FIGURE 1 · THE ENGAGEMENT: CLIENT, TYPE, REGULATORY STANDING AND THE REGULATOR THAT APPLIES**



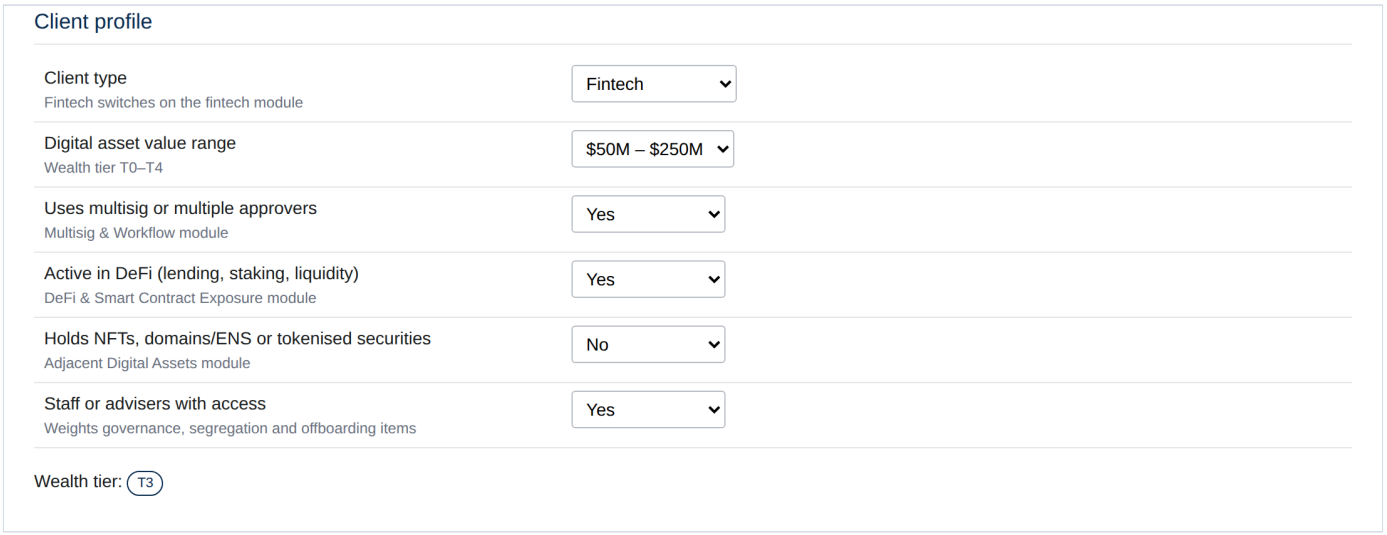

Source: DRA app 1.4.0, Overview page. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

Triage then asks what the firm does. Six core questions open the page; one of them, the digital asset value range, sets the wealth tier, and Meridian's *"$50M – $250M"* puts it at *T3*. The other five decide which modules apply. Eleven fintech ques-

© Olivier BUSOLINI - 2026 - No reuse without permission

tions follow, of which the jurisdictions and the value and client ranges set the operating profile, here *F2 Live, single jurisdiction* (content/rules.json and Triage page, DRA app 1.4.0). The bar the assessment measures against is the higher of the tier and the profile, which for this client is maturity level 3 on core risks and level 3 on the rest.

**FIGURE 2 · TRIAGE: THE ANSWERS THAT SET THE WEALTH TIER**

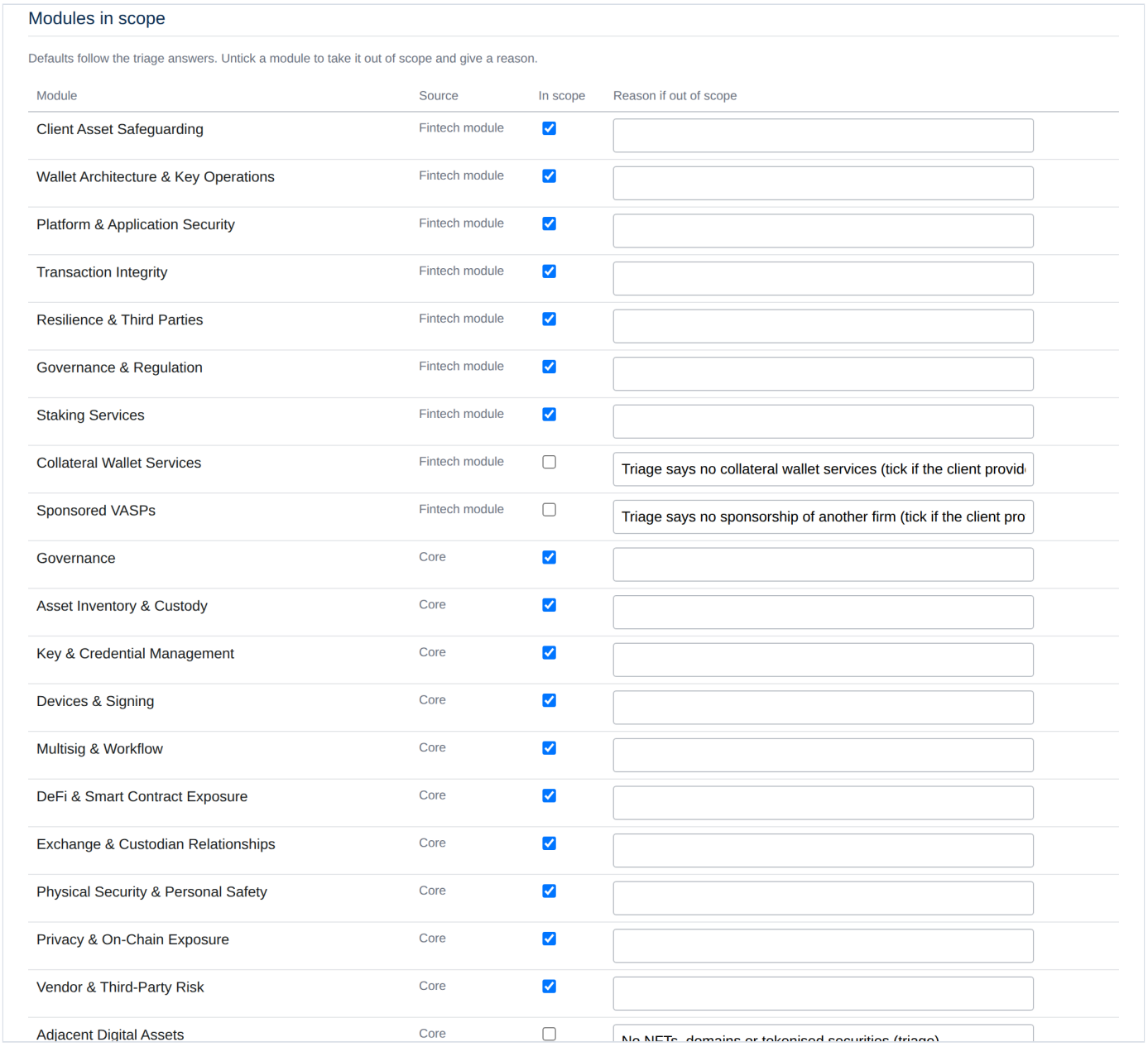



Source: DRA app 1.4.0, Triage page. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

The same answers decide what is asked at all. Three modules are taken out of scope because the triage says the firm neither holds collateral for a venue, nor sponsors another firm, nor holds NFTs, domains or tokenised securities. Nineteen of twenty-two modules remain, and the fieldwork drops from ninety-four questions to eighty-one (Figure 3). A module out of scope carries its reason on the page and in the report, so a client can see what was not examined and why.

© Olivier BUSOLINI - 2026 - No reuse without permission

## FIGURE 3 · WHICH MODULES APPLY TO THIS CLIENT, AND WHY THREE DO NOT



Modules in scope

Defaults follow the triage answers. Untick a module to take it out of scope and give a reason.

| Module | Source | In scope | Reason if out of scope |
|---|---|---|---|
| Client Asset Safeguarding | Fintech module | ☑ | |
| Wallet Architecture & Key Operations | Fintech module | ☑ | |
| Platform & Application Security | Fintech module | ☑ | |
| Transaction Integrity | Fintech module | ☑ | |
| Resilience & Third Parties | Fintech module | ☑ | |
| Governance & Regulation | Fintech module | ☑ | |
| Staking Services | Fintech module | ☑ | |
| Collateral Wallet Services | Fintech module | ☐ | Triage says no collateral wallet services (tick if the client provid |
| Sponsored VASPs | Fintech module | ☐ | Triage says no sponsorship of another firm (tick if the client pro |
| Governance | Core | ☑ | |
| Asset Inventory & Custody | Core | ☑ | |
| Key & Credential Management | Core | ☑ | |
| Devices & Signing | Core | ☑ | |
| Multisig & Workflow | Core | ☑ | |
| DeFi & Smart Contract Exposure | Core | ☑ | |
| Exchange & Custodian Relationships | Core | ☑ | |
| Physical Security & Personal Safety | Core | ☑ | |
| Privacy & On-Chain Exposure | Core | ☑ | |
| Vendor & Third-Party Risk | Core | ☑ | |
| Adjacent Digital Assets | Core | ☐ | No NFTs, domains or tokenised securities (triage) |

Source: DRA app 1.4.0, Triage page. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

© Olivier BUSOLINI - 2026 - No reuse without permission

# 2

# Interviews, drafted answers and the control assessment

Structured interviews, one session at a time, with every answer traceable to what was said.

The plan is built from the scope, not from a template: nine sessions, eighty-one questions.

A drafted answer carries no weight until the consultant accepts it.

A question the session never reached is left open, not filled in.

The interview plan is built from the scope, not from a template. For Meridian it comes to nine sessions over two days, eighty-one questions, fifty of them in band A, which is the set that must be asked in person. Each session names who should attend and what it covers; session F2, custody operations, is ninety minutes with the head of custody operations and the IT lead, and carries twelve questions (Figure 4).

© Olivier BUSOLINI - 2026 - No reuse without permission

## FIGURE 4 · THE INTERVIEW PLAN: ONE SESSION, WHO ATTENDS AND WHAT IT COVERS

Day 1 · Session 2 · 90 minutes · F2

Custody operations

Wallet structure, key operations, reconciliation and how a client transaction is actually executed.

**Expected:** Custody Operations, Chief Information Security Officer

Who attends

- [ ] Rashid Al Muhairi (BRD)
- [x] Sofia Almeida (OPS)
- [ ] Hassan Darwish (COMP)
- [x] Tomas Novak (CISO)

When: 09:00

| Item | Question | Band |
|---|---|---|
| **FIN-01** Client Asset Safeguarding | Client and company assets commingled · confirm in F1 | A only source for its risk |
| **FIN-02** Client Asset Safeguarding | Reconciliation weak or infrequent · confirm in F4 | A only source for its risk |
| **FIN-04** Client Asset Safeguarding | Dependence on a single custody or MPC provider · confirm in F1 | B supporting |
| **FIN-05** Wallet Architecture & Key Operations | Hot-wallet exposure uncontrolled | A core risk |
| **FIN-06** Wallet Architecture & Key Operations | Automated signer weakly protected · confirm in F3 | A core risk |
| **FIN-07** Wallet Architecture & Key Operations | Single or colluding operators can move funds | A core risk |
| **FIN-08** Wallet Architecture & Key Operations | Access not rotated after departures · confirm in F3 | A core risk |
| **FIN-09** Wallet Architecture & Key Operations | Wallet transfers weakly controlled | A core risk |
| **FIN-15** Transaction Integrity | Addresses not screened · confirm in F4 | A only source for its risk |
| **FIN-16** Transaction Integrity | Clients exposed to deposit and address fraud · confirm in F3 | B supporting |
| **FIN-17** Transaction Integrity | No procedure for network events · confirm in F3 | A only source for its risk |
| **FIN-25** Staking Services | Staking without a specific instruction · confirm in F4 | A core risk |

12 in scope, 10 in band A (9.0 minutes each).

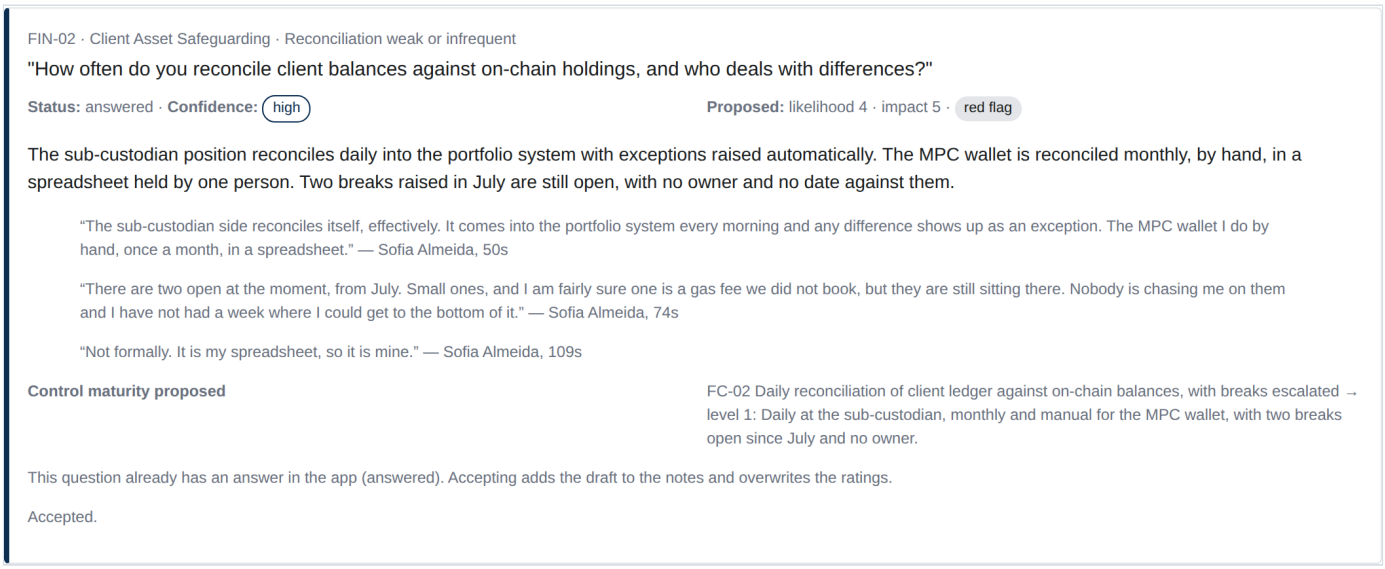
Source: DRA app 1.4.0, Interviews page. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

A session can be recorded, with consent, and transcribed; a transcript exported from Teams or Zoom is read directly and never leaves the consultant's machine. The AI assistant then drafts one answer per question from the transcript, quoting the speaker. The page is explicit about what that draft is worth: *"Nothing is scored until you accept it"*, and *"Every draft quotes the transcript; the import refuses a response whose quotes are not in the transcript"* (Extraction page, DRA app 1.4.0).

Figure 5 shows the draft for the reconciliation question. It quotes the head of custody operations three times, proposes a likelihood of 4 and an impact of 5, raises a red flag, and proposes a control maturity of level 1 with the reason drawn from what she said. The consultant accepted it. Of the twelve drafts from this session eleven were accepted and one was left open, because the session never reached the question: *"Bulk acceptance skips questions the interviews did not cover; those stay open for the follow-up"* (Extraction page, DRA app 1.4.0).

© Olivier BUSOLINI - 2026 - No reuse without permission

**FIGURE 5 · A DRAFTED ANSWER, QUOTED FROM THE TRANSCRIPT, AND THE DECISION ON IT**




Source: DRA app 1.4.0, Extraction page. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

The Fieldwork page shows where the assessment has got to, module by module, with the red flags counted (Figure 6). Each question has its own entry: what to capture, what the red flags are, the risk it feeds, the scores, who answered it and what they said (Figure 7).

© Olivier BUSOLINI - 2026 - No reuse without permission

**FIGURE 6 · FIELDWORK PROGRESS BY MODULE, WITH RED FLAGS COUNTED**

## Fieldwork

### Immediate triggers

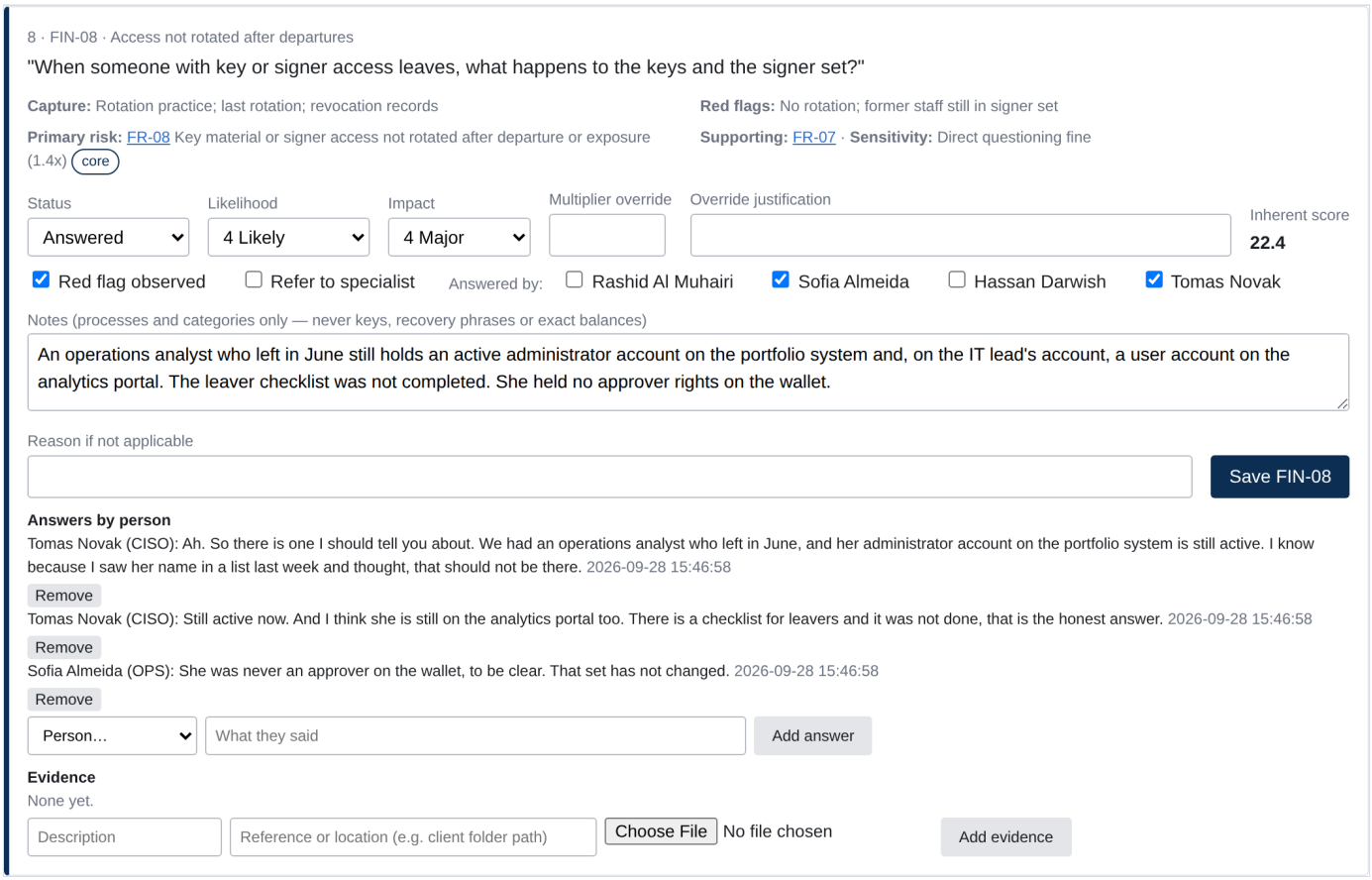
- Blind signing while actively using DeFi or NFTs (DEV-02)
- Former staff still hold keys or signer rights (FIN-08)
- Unresolved reconciliation breaks on client assets (FIN-02)

| Module | Source | Questions | Done | Deferred | Red flags | Scope |
|---|---|---|---|---|---|---|
| Client Asset Safeguarding | Fintech | 4 | 4 | 0 | 1 | In scope |
| Wallet Architecture & Key Operations | Fintech | 5 | 5 | 0 | 1 | In scope |
| Platform & Application Security | Fintech | 5 | 5 | 0 | 0 | In scope |
| Transaction Integrity | Fintech | 3 | 3 | 0 | 0 | In scope |
| Resilience & Third Parties | Fintech | 3 | 3 | 0 | 0 | In scope |
| Governance & Regulation | Fintech | 4 | 4 | 0 | 0 | In scope |
| Staking Services | Fintech | 5 | 5 | 0 | 0 | In scope |
| Collateral Wallet Services | Fintech | 3 | 0 | 0 | 0 | Out of scope: Triage says no collateral wallet services (tick if the client provides it) |
| Sponsored VASPs | Fintech | 2 | 0 | 0 | 0 | Out of scope: Triage says no sponsorship of another firm (tick if the client provides it) |
| Governance | Core | 3 | 3 | 0 | 0 | In scope |
| Asset Inventory & Custody | Core | 4 | 4 | 0 | 0 | In scope |
| Key & Credential Management | Core | 6 | 6 | 0 | 0 | In scope |
| Devices & Signing | Core | 7 | 7 | 0 | 1 | In scope |
| Multisig & Workflow | Core | 5 | 5 | 0 | 0 | In scope |
| DeFi & Smart Contract Exposure | Core | 5 | 5 | 0 | 0 | In scope |
| Exchange & Custodian Relationships | Core | 5 | 5 | 0 | 0 | In scope |
| Physical Security & Personal Safety | Core | 4 | 4 | 0 | 0 | In scope |
| Privacy & On-Chain Exposure | Core | 3 | 3 | 0 | 0 | In scope |
| Vendor & Third-Party Risk | Core | 4 | 4 | 0 | 0 | In scope |

Source: DRA app 1.4.0, Fieldwork page. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

© Olivier BUSOLINI - 2026 - No reuse without permission

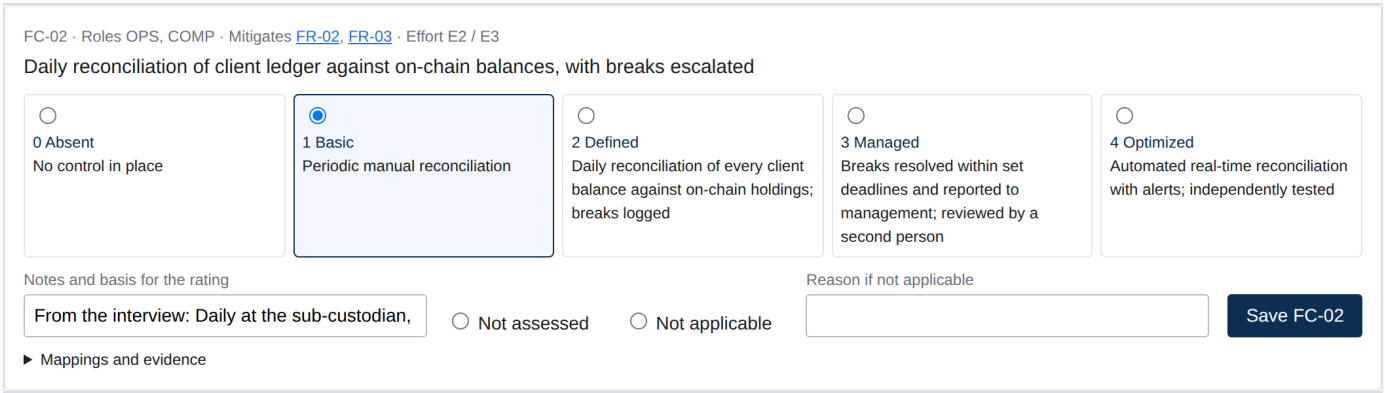
## FIGURE 7 · ONE QUESTION: GUIDANCE, THE ANSWER WITH ITS QUOTES, AND THE SCORES




Source: DRA app 1.4.0, Wallet Architecture & Key Operations page. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

Answers describe what happens; controls describe what protects against it. The Controls page carries a maturity ladder for each of the eighty-five controls, and the consultant records the level the evidence supports. The page states the rule that makes the ladder matter: *"A risk takes the lowest maturity among its mapped controls. Leave a control unassessed until you have the evidence"* (Controls page, DRA app 1.4.0). For this client sixty-three controls were assessed and twenty-two marked not applicable, each with a reason.

## FIGURE 8 · ONE CONTROL: THE MATURITY LADDER AND THE LEVEL RECORDED




Source: DRA app 1.4.0, Controls page. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

© Olivier BUSOLINI - 2026 - No reuse without permission

# 3

# What the assessment finds

One register for the engagement, scored from the answers, with the urgent findings raised first.

The arithmetic is published, so a client can check a score instead of taking it on trust.

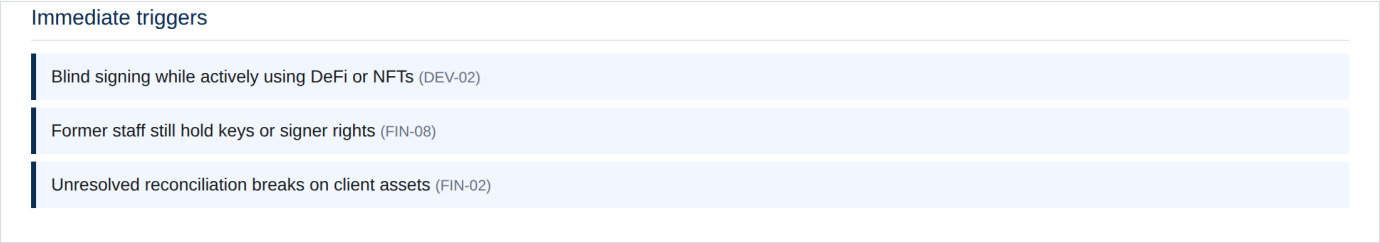
Three findings are raised with the client ahead of the report.

Only five of the sixty-eight risks already meet the bar this client is held to.

The score is arithmetic and the arithmetic is published. Inherent risk is *"likelihood * impact * multiplier"*, where the multiplier reflects how irreversible the loss would be. Residual risk is *"inherent * (1 - maturity_reduction[maturity])"*, with the reduction running 0 per cent at level 0, then 20, 40, 65 and 85 per cent. A risk takes *"the lowest maturity among the controls mapped to the risk; consultant override requires a written justification"*, and the bands are Low up to 6, Medium to 12, High to 20 and Critical above that (content/rules.json, DRA app 1.4.0, citing Framework Sections 4 and 7).

Three findings do not wait for the report. The framework asks for urgent findings to be raised with the client first, and the application lists them at the top of the Results page: blind signing while the firm is active in DeFi, a former member of staff still holding access, and unresolved reconciliation breaks on client assets (Figure 9). The first fires because triage records the firm as *"Active in DeFi (lending, staking, liquidity)"*, which for Meridian means staking (content/rules.json and Triage page, DRA app 1.4.0). Each finding is tied to the question that raised it, so the client sees what was said and not only what was concluded.

**FIGURE 9 · THE THREE FINDINGS THAT CANNOT WAIT FOR THE REPORT**




Source: DRA app 1.4.0, Results page. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

Sixty-eight risks were scored for this client: four Critical, twenty High, twenty-nine Medium and fifteen Low, with the maturity target met on five (Results page, DRA app 1.4.0). The register lists them by residual score, with the inherent score, the maturity counted and the gap against the target beside each one, so a client can see whether a high score comes from the exposure or from the absence of protection (Figure 10).

© Olivier BUSOLINI - 2026 - No reuse without permission

**FIGURE 10 · THE RISK REGISTER, HIGHEST RESIDUAL FIRST**

Risk register

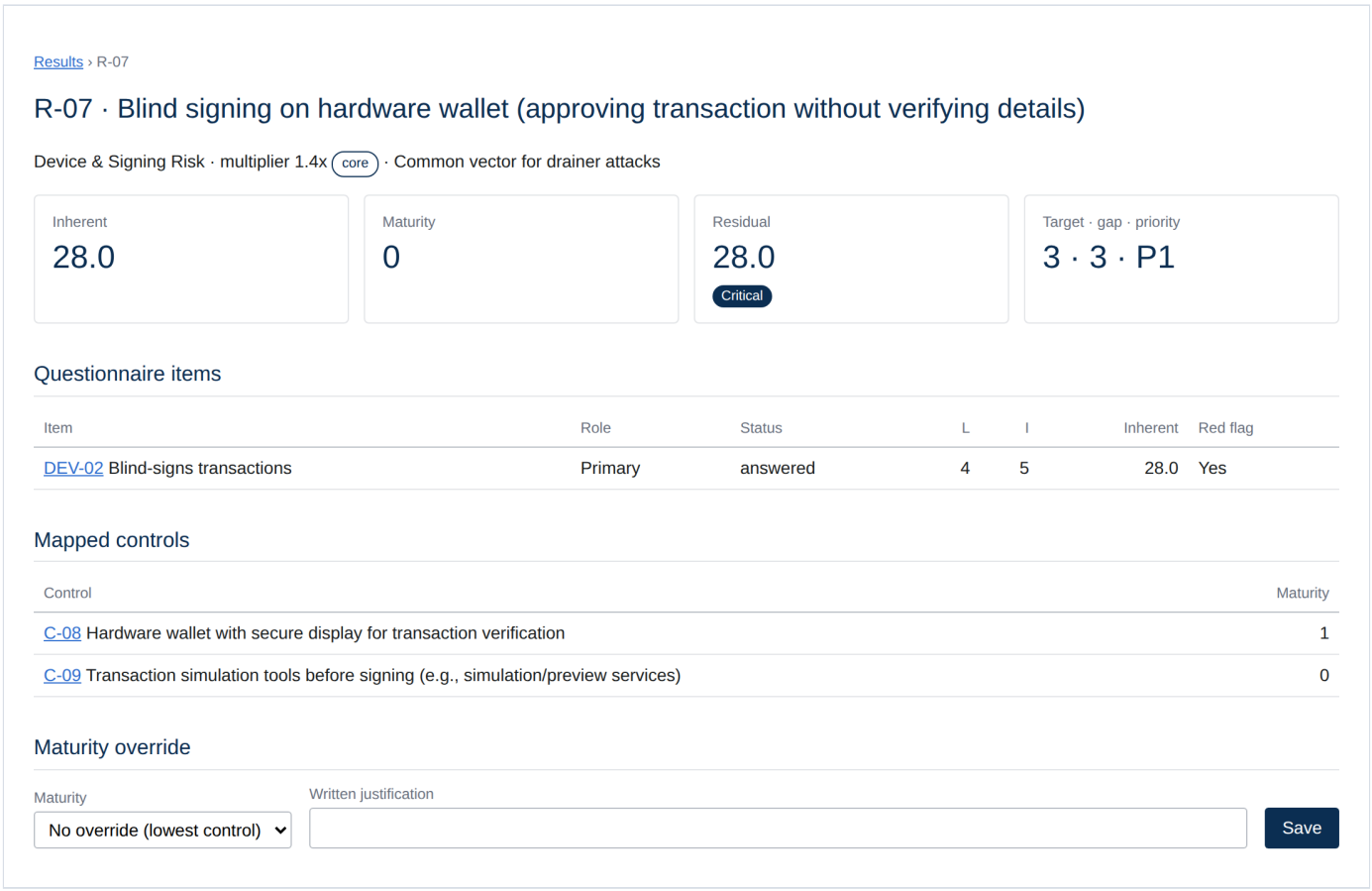
| ID | Risk | Inherent | Maturity | Residual | Rating | Target | Gap | Priority |
|---|---|---|---|---|---|---|---|---|
| R-07 | Blind signing on hardware wallet (approving transaction without verifying details) core | 28.0 | 0 | 28.0 | Critical | 3 | 3 | P1 |
| FR-02 | Reconciliation failure (client ledger does not match on-chain balances) | 26.0 | 0 | 26.0 | Critical | 3 | 3 | P1 |
| FR-11 | Application or API vulnerability enabling unauthorised withdrawals or balance changes core | 23.2 | 0 | 23.2 | Critical | 3 | 3 | P1 |
| R-06 | Compromised computer/phone used for transaction signing core | 22.4 | 0 | 22.4 | Critical | 3 | 3 | P1 |
| FR-21 | Security governance inadequate for regulated activity | 19.2 | 0 | 19.2 | High | 3 | 3 | P1 |
| R-01 | Seed phrase/private key loss (no backup or backup destroyed) core | 24.0 | 1 | 19.2 | High | 3 | 2 | P1 |
| FR-08 | Key material or signer access not rotated after departure or exposure core | 22.4 | 1 | 17.92 | High | 3 | 2 | P1 |
| R-14 | Collusion risk among signers core (from supporting items) | 22.4 | 1 | 17.92 | High | 3 | 2 | P1 |
| FR-16 | Deposit and withdrawal fraud (address poisoning of clients, false deposits) | 21.6 | 1 | 17.28 | High | 3 | 2 | P1 |
| R-46 | Inadequate offboarding (former staff retain access) | 21.6 | 1 | 17.28 | High | 3 | 2 | P1 |
| R-51 | Inadequate incident response (no plan for suspected key compromise) | 21.6 | 1 | 17.28 | High | 3 | 2 | P1 |
| FR-12 | Cloud or infrastructure misconfiguration exposing systems or secrets | 16.2 | 0 | 16.2 | High | 3 | 3 | P1 |
| R-12 | Signer geographic/custodial concentration (all keys in one location) | 19.5 | 1 | 15.6 | High | 3 | 2 | P1 |
| R-29 | Loss/damage from disaster (fire, flood) without geographic redundancy (from supporting items) | 19.5 | 1 | 15.6 | High | 3 | 2 | P1 |
| R-13 | Signer unavailability risk (key holder incapacitated, unreachable) | 19.2 | 1 | 15.36 | High | 3 | 2 | P1 |
| FR-18 | Failure or concentration of a critical outsourced provider (cloud, custody technology, KYC) | 18.0 | 1 | 14.4 | High | 3 | 2 | P1 |
| R-10 | Lack of transaction simulation/verification tooling | 14.4 | 0 | 14.4 | High | 3 | 3 | P1 |

Source: DRA app 1.4.0, Results page. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

The first row is blind signing on a signing device, at 28.0. Its own page shows how the number is built: the questions that feed it, the controls mapped to it, the lowest of their maturities and the reduction that follows (Figure 11). Nothing about the calculation is hidden from the client, which matters when the conversation turns to whether a finding is fair.

© Olivier BUSOLINI - 2026 - No reuse without permission

## FIGURE 11 · ONE RISK: HOW THE SCORE IS BUILT, AND WHICH CONTROLS LIMIT IT




Source: DRA app 1.4.0, Results — one risk page. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

© Olivier BUSOLINI - 2026 - No reuse without permission

# 4

# What to do, and in what order

Priority and urgency are derived from the rules; the consultant's judgement is recorded, not hidden.

The AI assistant may raise a calculated priority, and may never lower it.

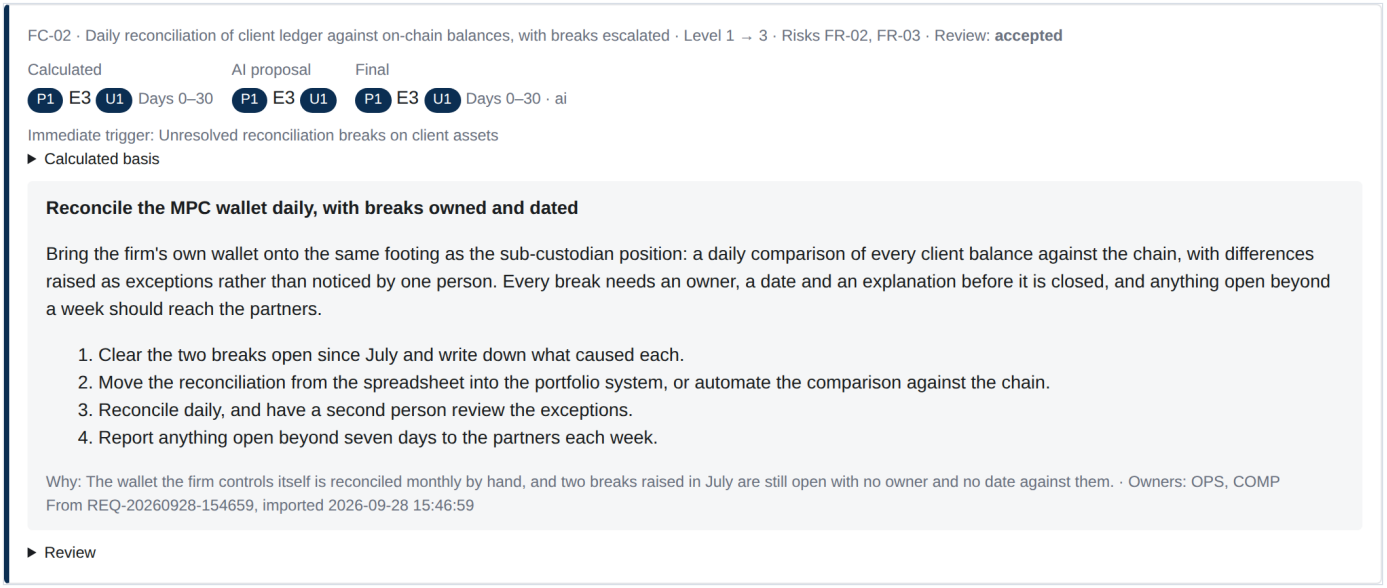
Every recommendation is reviewed, and an edit or a rejection needs a written reason.

The first window is heavy, and that is the answer rather than a number to soften.

Every gap between a control's current level and its target produces a recommendation, with a priority and an urgency the rules derive rather than the consultant chooses. Priority P1 is a Critical risk, or a High risk with a gap of two levels or more. Urgency U1 is anything tied to an immediate trigger, or a P1 on a core risk that takes little effort, and its actions *"start_within_days: 7"* (content/rules.json, DRA app 1.4.0, citing Framework Sections 9.1 and 9.3).

For Meridian that produced fifty-five recommendations: forty at P1 and fourteen at P2 among those that reached the report, with nine at U1. Twenty carried wording drafted by the AI assistant. Figure 12 shows one of them: the calculated values, the assistant's proposal, the consultant's final values and the wording the client will read. The assistant *"can raise a calculated priority or urgency but never lower it"*, and the consultant reviews every draft (AI drafts page, DRA app 1.4.0).

**FIGURE 12 · A RECOMMENDATION: THE CALCULATION, THE DRAFTED WORDING AND THE REVIEW**



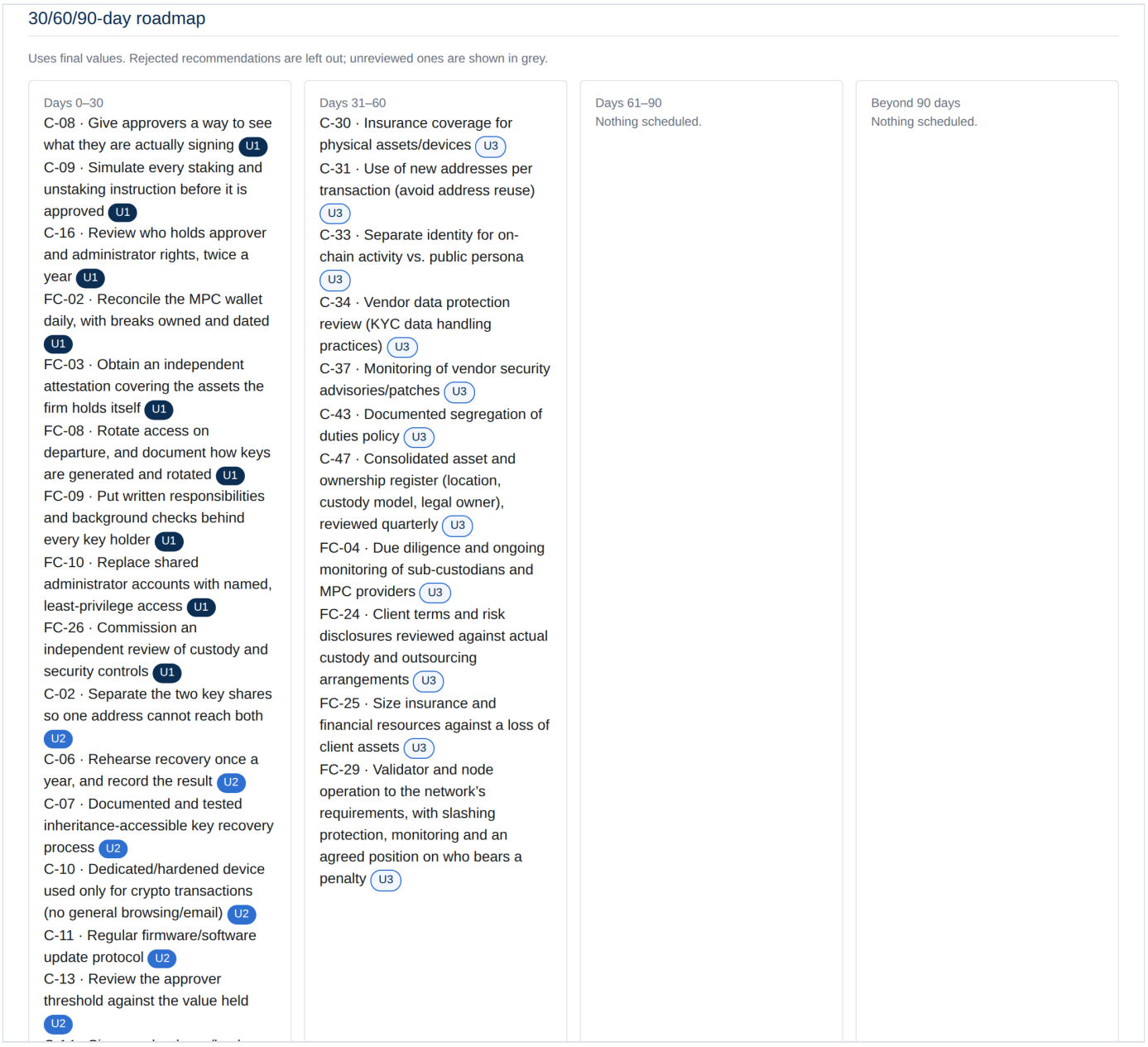

Source: DRA app 1.4.0, Results page. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

The review is where judgement enters, and it is recorded. Of the fifty-five, fifty-one were accepted as drafted, three were edited and one was rejected. The rejection was the recommendation for an air-gapped signing device, rejected because this client's architecture has no signing device to air-gap; the reason is stored with the decision and appears in the report. An edit or a rejection without a reason is refused.

The roadmap turns the priorities into dates, in four windows (Figure 13). Forty-three actions fall in the first thirty days and eleven in the next thirty (report 1.0, Meridian Gulf Family Office). That is a heavy first window for a firm of fourteen people, and it is the honest output of a licensed firm measured against level 3: it is the conversation the assessment is meant to start, not a number to be softened.

© Olivier BUSOLINI - 2026 - No reuse without permission

**FIGURE 13 · THE ROADMAP, WINDOW BY WINDOW; THE FIRST LIST IS LONGER THAN THE FIGURE**




Source: DRA app 1.4.0, Results page. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

Not everything belongs in the register. The Follow-ups page collects *"Everything that is still open, deferred, referred or excluded, in one place"* (Follow-ups page, DRA app 1.4.0): two deferred questions on the firm's own succession, and five specialist referrals where the right answer is a lawyer, a broker or a penetration tester and not a recommendation (Figure 14). Further down the same page sit the modules and controls taken out of scope, each with its reason.

© Olivier BUSOLINI - 2026 - No reuse without permission

## FIGURE 14 · FOLLOW-UPS: DEFERRED QUESTIONS AND SPECIALIST REFERRALS

### Deferred questions

| Question | Topic | Module |
|---|---|---|
| INH-02 | No documented succession plan | Inheritance & Succession (Flag-and-Refer Only) |
| INH-03 | No specialized estate counsel engaged | Inheritance & Succession (Flag-and-Refer Only) |

### Specialist referrals

| Specialist | Reason |
|---|---|
| Estate counsel with digital asset experience | Succession and recovery arrangements need legal structuring (R-52, C-07, C-49). |
| Executive protection adviser | Exposure to coercion or targeting warrants a personal security review (R-27). |
| Regulatory counsel | Licence scope, security obligations or client terms need review (FR-22, FR-23). |
| Insurance broker | Insurance and capital for client asset loss need sizing (FR-24). |
| Independent penetration tester | The platform has not been tested independently to the expected level (FC-13). |

Source: DRA app 1.4.0, Follow-ups page. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

© Olivier BUSOLINI - 2026 - No reuse without permission

# 5

# What the client receives

A report that is refused until the assessment is complete, kept as issued, and compared next time.

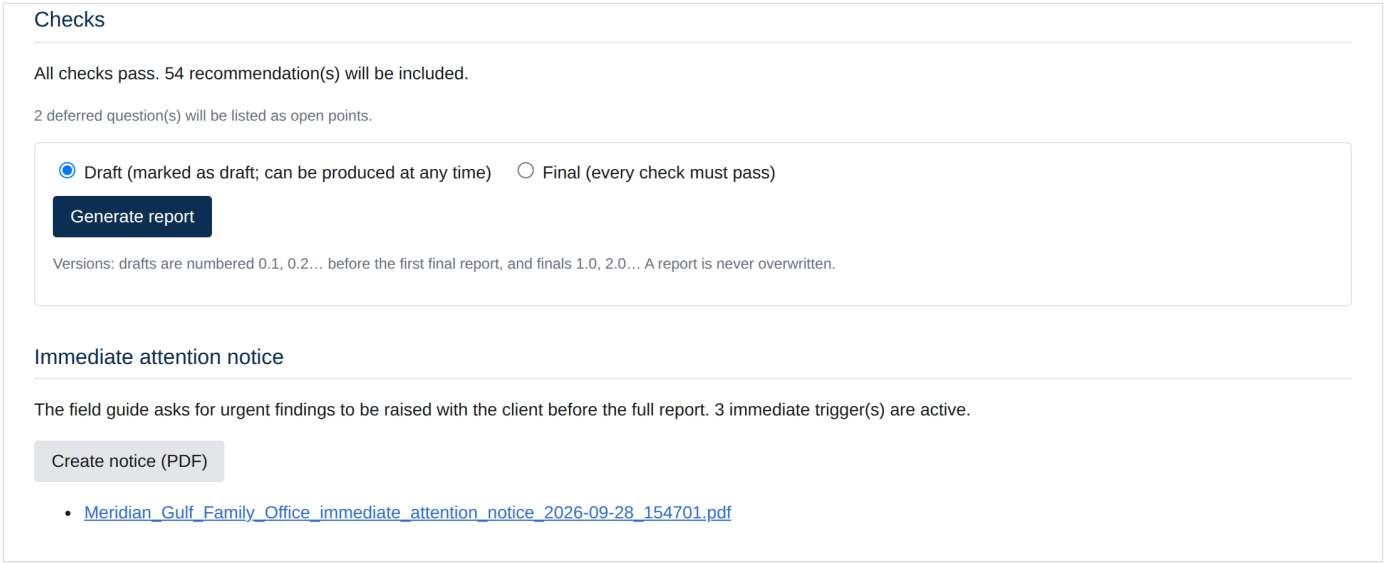
A draft report can be produced at any time; a final cannot.

Each version is filed with a fingerprint and the data behind it, and never overwritten.

The second engagement starts from the first report's snapshot, not from nothing.

A final report cannot be produced until the assessment is complete. Six checks stand between the consultant and the button: the client named, the tier set, the operating profile set, every recommendation reviewed, no drafts out of date against a changed calculation, and at least one recommendation accepted. Any that fails is named on the page with what to do about it; Figure 15 is the other case, where the page reports only *"All checks pass"* and the count it will include (dra/__init__.py, report_checks; Report page, DRA app 1.4.0). A draft report can be produced at any time; a final cannot.

**FIGURE 15 · THE CHECKS A FINAL REPORT HAS TO PASS**




Source: DRA app 1.4.0, Report page. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

What the client receives is a PDF in the same document style as this one, carrying only accepted and edited recommendations, together with an immediate attention notice for the three findings that could not wait. Report 1.0 for this client ran to forty-eight pages and fifty-four recommendations. Each version is filed unchanged with a fingerprint and the data behind it: *"drafts are numbered 0.1, 0.2… before the first final report, and finals 1.0, 2.0… A report is never overwritten"* (Report page, DRA app 1.4.0). Figure 16 shows version 1.0 as issued and the 1.1 draft produced after the client had made changes.

© Olivier BUSOLINI - 2026 - No reuse without permission

**FIGURE 16 · REPORT VERSIONS, EACH KEPT AS ISSUED WITH ITS FINGERPRINT**

Versions

| Version | Status | Created | Pages | Recommendations | Fingerprint (SHA-256) | |
|---|---|---|---|---|---|---|
| 1.1 | draft | 2026-09-28 15:47:31 | 52 | 51 | 33061ae6d3224201… | PDF · Data |
| 1.0 | final | 2026-09-28 15:47:01 | 48 | 54 | b8963fdc94db5a39… | PDF · Data |

Source: DRA app 1.4.0, Report page. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

A later assessment compares against any earlier report. Set against version 1.0, the test client shows *"6 risk(s) improved, 0 slipped, 62 unchanged"* and *"4 control(s) rated higher, 0 lower"*, and of the fifty-four recommendations made then, three are met and one has progressed (Reassessment page, DRA app 1.4.0). That is the page a client sees at the second engagement, and it is the reason the first one is worth doing properly: the register becomes a baseline instead of a document.

**FIGURE 17 · REASSESSMENT: WHAT MOVED SINCE REPORT 1.0**

Since Meridian Gulf Family Office v1.0, 2026-09-28 15:47:01

6 risk(s) improved, 0 slipped, 62 unchanged. 4 control(s) rated higher, 0 lower. Of 54 recommendation(s) made then: 3 met, 1 progressed, 50 untouched, 0 worse.

What happened to the last recommendations

| Control | Then | Now | Maturity | State |
|---|---|---|---|---|
| C-06 Regular key ceremony audits (verify all signers/backups functional) | P1 | P1 | 1 → 1 | untouched |
| C-07 Documented and tested inheritance-accessible key recovery process | P1 | P1 | 2 → 2 | untouched |
| C-08 Hardware wallet with secure display for transaction verification | P1 | P1 | 1 → 1 | untouched |
| C-09 Transaction simulation tools before signing (e.g., simulation/preview services) | P1 | P1 | 0 → 0 | untouched |
| C-10 Dedicated/hardened device used only for crypto transactions (no general browsing/email) | P1 | P1 | 0 → 0 | untouched |
| C-11 Regular firmware/software update protocol | P1 | P1 | 2 → 2 | untouched |
| C-13 Defined signer threshold appropriate to wealth tier | P1 | P1 | 2 → 2 | untouched |
| C-14 Signer redundancy/backup signer designation | P1 | P1 | 1 → 1 | untouched |
| C-15 Documented approval workflow (segregation of initiator/approver) | P1 | P1 | 2 → 2 | untouched |
| C-16 Periodic signer access review | P1 | P1 | 1 → 1 | untouched |
| C-17 Due diligence checklist before interacting with new protocols (audit status, TVL, track record) | P1 | P1 | 1 → 1 | untouched |
| C-20 Diversification across multiple custodians/exchanges (no single point of concentration) | P1 | P1 | 1 → 1 | untouched |
| C-21 Qualified custodian due diligence (insurance, audit reports, regulatory status) | P1 | P1 | 2 → 2 | untouched |
| C-27 Bank vault or professional vault storage for cold storage backups | P1 | P2 | 2 → 2 | untouched |
| C-28 Operational security training (avoid public disclosure of holdings) | P1 | P1 | 1 → 1 | untouched |
| C-29 Duress/coercion protocol (decoy wallet, silent alarm procedures) | P1 | P1 | 0 → 0 | untouched |
| C-35 Formal vendor due diligence and approval process | P1 | P1 | 2 → 2 | untouched |
| C-36 Vendor concentration limits (no single vendor holding majority of assets) | P1 | P1 | 1 → 1 | untouched |
| C-45 Business continuity plan with designated backup decision-makers | P1 | P1 | 2 → 2 | untouched |
| C-48 Documented and rehearsed incident response plan, including a key-compromise playbook | P1 | P1 | 1 → 1 | untouched |
| FC-01 Client assets segregated from company assets in separate, labelled wallets and records | P1 | P1 | 2 → 2 | untouched |
| FC-03 Proof of reserves or independent attestation of client assets | P1 | P1 | 2 → 2 | untouched |
| FC-09 Personnel security for key holders (background checks, written responsibilities, training) | P1 | P1 | 2 → 2 | untouched |
| FC-10 Privileged access management for production and wallet systems, with quarterly access reviews | P1 | P1 | 1 → 1 | untouched |

Source: DRA app 1.4.0, Reassessment page. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

© Olivier BUSOLINI - 2026 - No reuse without permission

# 6

# How the client's material is handled

What leaves the consultant's machine, what never does, and what is recorded.

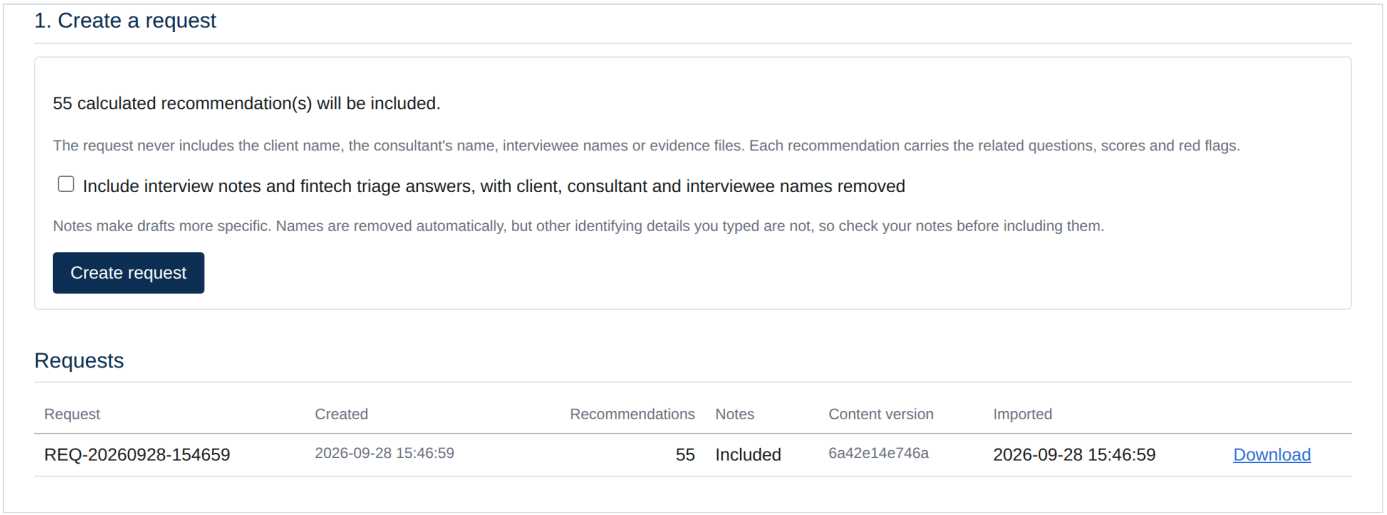
The extraction step needs the words, so it carries names; the recommendation step does not.

The audit log is a check, not a lock, and the application says so.

The application runs on the consultant's own machine, on the loopback address, with one folder per client. Two things leave it, and the difference between them is deliberate.

A recording, if a session was recorded, goes to a transcription service and is deleted from it as soon as the text returns; a transcript exported from Teams or Zoom never leaves at all. The extraction that follows has to quote the client word for word, so it carries the transcript with the real names in it. The recommendation step is different: it needs the findings, not the people. The page states what the request contains: *"The request never includes the client name, the consultant's name, interviewee names or evidence files. Each recommendation carries the related questions, scores and red flags"*, and where notes are included, *"Names are removed automatically, but other identifying details you typed are not, so check your notes before including them"* (AI drafts page, DRA app 1.4.0).

**FIGURE 18 · THE REQUEST TO THE AI ASSISTANT, AND WHAT IT CONTAINS**




Source: DRA app 1.4.0, AI drafts page. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

Every action is recorded. The audit log for this assessment held two hundred and ninety-two entries when these screens were taken, and states plainly both what it does and what it does not: *"Each entry carries a fingerprint of itself and of the one before it, so an entry edited or removed outside the app would show here. It is a check, not a lock: anyone who can open the client folder can still change the file"* (Audit log page, DRA app 1.4.0).

© Olivier BUSOLINI - 2026 - No reuse without permission

**FIGURE 19 · THE AUDIT LOG, MOST RECENT ENTRIES, EACH CHAINED TO THE ONE BEFORE**

## Audit log

292 entries, chained. Each entry carries a fingerprint of itself and of the one before it, so an entry edited or removed outside the app would show here. It is a check, not a lock: anyone who can open the client folder can still change the file.

| When | Who | Action | Subject | Detail |
|---|---|---|---|---|
| 2026-09-28 15:47:03 | claude | login | session | second factor verified |
| 2026-09-28 15:47:02 | — | password reset | users | claude, by the screen capture script |
| 2026-09-28 15:47:02 | claude | baseline set | reassessment | version 1.0 of Meridian Gulf Family Office, created 2026-09-28 15:47:01 |
| 2026-09-28 15:47:02 | claude | report | version 1.0 | final; 48 pages; sha256 b8963fdc94db5a39 |
| 2026-09-28 15:47:01 | claude | notice | immediate attention | 3 finding(s); Meridian_Gulf_Family_Office_immediate_attention_notice_2026-09-28_154701.pdf |
| 2026-09-28 15:47:00 | claude | review | recommendation FC-29 | accepted; ; |
| 2026-09-28 15:47:00 | claude | review | recommendation FC-25 | accepted; ; |
| 2026-09-28 15:47:00 | claude | review | recommendation FC-24 | accepted; ; |
| 2026-09-28 15:47:00 | claude | review | recommendation FC-04 | accepted; ; |
| 2026-09-28 15:47:00 | claude | review | recommendation C-47 | accepted; ; |
| 2026-09-28 15:47:00 | claude | review | recommendation C-43 | accepted; ; |
| 2026-09-28 15:47:00 | claude | review | recommendation C-37 | accepted; ; |
| 2026-09-28 | claude | review | recommendation C-34 | accepted; ; |

Source: DRA app 1.4.0, Audit log page. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

At the end of an engagement the client folder is closed: an encrypted backup is written and verified, and the working material is removed. The client keeps the report, and the next engagement starts from its snapshot, not from nothing.

© Olivier BUSOLINI - 2026 - No reuse without permission

# 7

# Sources

## The documents and pages this one draws on.

The framework, the questionnaire and the application are the author's own. The standards and rulebooks the framework maps to are public, and every citation in the application is verified against the primary text, dated, and re-checked twice a year.


1 Digital asset risk assessment framework v2, and the fintech module v1 (available on request)

2 Digital asset risk assessment questionnaire v2 (available on request)

3 DRA app 1.4.0: the screens of Meridian Gulf Family Office (fictitious), captured 28 September 2026

4 DRA app 1.4.0: the assessment's own rules file, content/rules.json, content version 6a42e14e746a

5 DRA app — User guide, and DRA app — Architecture map 1.4.0

6 CryptoCurrency Security Standard v9, CryptoCurrency Certification Consortium https://cryptoconsortium.org/cryptocurrency-security-standard-ccss/

7 NIST Cybersecurity Framework 2.0 https://www.nist.gov/cyberframework

8 VARA Technology and Information Rulebook https://rulebooks.vara.ae/rulebook/technology-and-information-rulebook

9 VARA Custody Services Rulebook https://rulebooks.vara.ae/rulebook/custody-services-rulebook

10 VARA Company Rulebook https://rulebooks.vara.ae/rulebook/company-rulebook

11 VARA Compliance and Risk Management Rulebook https://rulebooks.vara.ae/rulebook/compliance-and-risk-management-rulebook

12 VARA Market Conduct Rulebook https://rulebooks.vara.ae/rulebook/market-conduct-rulebook


© Olivier BUSOLINI - 2026 - No reuse without permission

# Appendix A · The screens in this tour

TABLE 1 · SCREENS SHOWN, IN ORDER

| FIGURE | SCREEN | WHAT IT SHOWS |
|---|---|---|
| **Figure 1** | Overview | The engagement: client, type, regulatory standing and regulator |
| **Figure 2** | Triage | The answers that set the wealth tier |
| **Figure 3** | Triage | Modules in scope, and the reason where one is not |
| **Figure 4** | Interviews | One session of the plan: who attends and what it covers |
| **Figure 5** | Extraction | A drafted answer with its quotes, and the decision on it |
| **Figure 6** | Fieldwork | Progress by module, with red flags counted |
| **Figure 7** | Fieldwork, one module | One question: guidance, answer, quotes and scores |
| **Figure 8** | Controls | One control: the maturity ladder and the level recorded |
| **Figure 9** | Results | The immediate triggers |
| **Figure 10** | Results | The risk register |
| **Figure 11** | Results, one risk | How one risk's score is built |
| **Figure 12** | Results | A recommendation, its drafted wording and its review |
| **Figure 13** | Results | The 30/60/90-day roadmap, window by window |
| **Figure 14** | Follow-ups | Deferred questions and specialist referrals |
| **Figure 15** | Report | The report page with every check passing |
| **Figure 16** | Report | Report versions |
| **Figure 17** | Reassessment | What changed since report 1.0 |
| **Figure 18** | AI drafts | The request and what it contains |
| **Figure 19** | Audit log | The chained record of actions |

DRA app 1.4.0. Meridian Gulf Family Office (fictitious), test data, 28 September 2026.

# Appendix B · How this tour was prepared

## B.1 The client is fictitious

Meridian Gulf Family Office does not exist. The firm, the four people, the custody arrangement, the departed analyst, the reconciliation breaks and every answer were invented to exercise the application. The Overview page of the folder records the scope as a fictitious client prepared to illustrate the application, with no real client, no real answer and no real finding.

## B.2 How the assessment was completed

The folder was prepared with the application's own tool, tools/prep_test_client.py, run with the full stage, which enters every answer, control maturity, review, notice and

© Olivier BUSOLINI - 2026 - No reuse without permission

report through the application's own pages and not into the database behind it, so the capability checks, the cross-site request checks and the audit log all saw it as they would see a consultant working by hand. A fictitious thirty-four turn transcript of session F2 was filed as a meeting transcript, which needs no transcription service, and the answer extraction was run over it, so that the drafted answers in Figures 5 and 7 quote a real transcript and not an invented one.

## B.3 How the screens were captured

The screens were captured with tools/capture_screens.py on DRA app 1.4.0 on 28 September 2026, in Chromium at a width of 1,100 pixels and twice the usual pixel density, signed in as a lead consultant. Each figure is a region of one page, cut at a heading or block boundary, and then capped in height so that no figure runs longer than a page: Figures 3, 13, 17 and 19 are trimmed, and each continues below the edge shown. The page footer, which carries the version and the data folder, and the status strip, which carries whatever the last action happened to say, are hidden. Figures 16 and 17 were captured after a second pass in which the client fixed four things; the other seventeen show the assessment exactly as the client received it, with all three immediate triggers still open.

## B.4 Where the figures in the text come from

Every figure quoted in the body is read from the screen shown, or from the assessment's own rules file, content/rules.json, which names the framework section each rule applies. Quoted page wording is reproduced exactly. No statement in this document rests on an unnamed source.

© Olivier BUSOLINI - 2026 - No reuse without permission