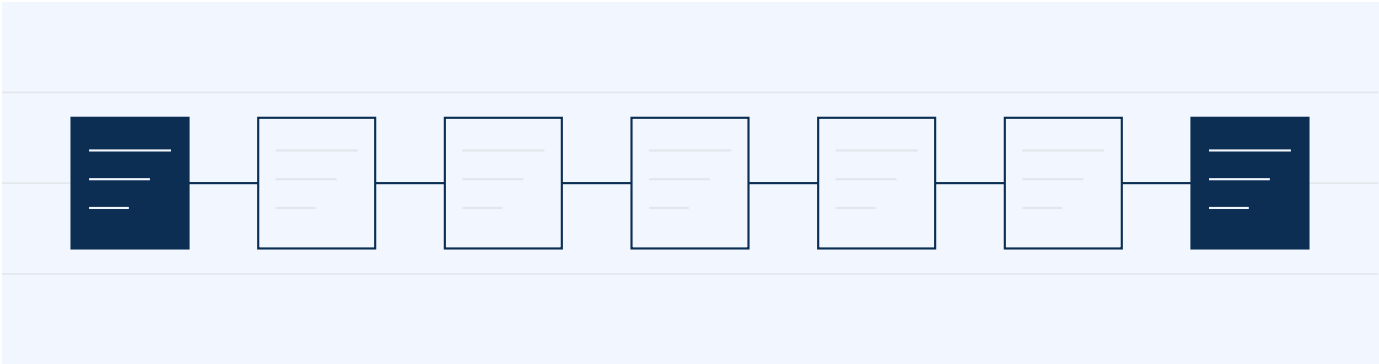
SERVICE TOUR

Inside a VIP digital life protection assessment

A tour of the assessment app on a fictitious household, from the first interview to the reports the family receives.



DATE	AUDIENCE	FORMAT	VERSION
26 September 2026	Principals and family offices	Illustrated walkthrough	1.0

Olivier Busolini

© Olivier BUSOLINI - 2026 - No reuse without permission

Contents

This document walks through one complete assessment in the VIP app, the tool that runs a digital life protection engagement for a family. The household is fictitious: the Haddads, a principal, his spouse, their daughter and two members of staff, prepared as test data so that every screen carries realistic content without describing a real person. The tour follows the order of the work. It opens with the household register, where each person receives their own tier, then covers the interviews, the drafted answers and the hands-on checks, then what the assessment finds and what it recommends, in what order. It shows what the family receives: an engagement report for the principal, a short report for each person and a notice for findings that cannot wait. The last section shows how the family's material is protected: the restricted file for safety matters, pseudonymised requests to the AI assistant, a chained audit log and the closing of the file. Seventeen screens illustrate the tour; Appendix A lists them and Appendix B records how the test household was prepared.

01	The household, person by person	4
02	Interviews, drafted answers and checks	5
03	What the assessment finds	8
04	What to do, and in what order	11
05	What the family receives	13
06	How the family's material is protected	16
07	Sources	19
A	Appendix A: The screens in this tour	20
B	Appendix B: How this tour was prepared	21

© Olivier BUSOLINI - 2026 - No reuse without permission

Executive summary

- **Every person in the household is assessed in their own right.** The Haddad register holds five people; the executive assistant sits at T4 with the principal because he holds delegated access to the principal's accounts (Figure 1).
- **The interviews follow a fixed plan, one person at a time.** Eleven sessions cover 156 questions: scoping, shared arrangements, one session per person, the hands-on checks and a closing session (Figure 3).
- **Nothing is scored from a transcript until the consultant accepts it.** Each drafted answer quotes the interview word for word, and the app refuses a quote that is not in the transcript (Figure 4).
- **A protection level the family states counts one level lower until it is checked.** A hands-on check, with the person's written consent, lets the level count in full (content/rules.json, citing Framework v4 Sections 4.8 and 8; Checks page).
- **The register scores each risk at the person who carries the most of it.** In the test household 8 risks are Critical and 19 High; the most severe is a payment made on a fake instruction, at 24.0 (Figure 8).
- **Every recommendation shows three levels, the residual risk at each and the cost in daily life.** The family chooses with the trade-off in view (Figure 10).
- **Actions are sequenced into a 90-day plan.** Thirty actions fall in the first 30 days; the five marked U1, the most urgent, start within 7 days (Figure 11; content/rules.json, citing Framework v4 Section 9.3).
- **The family receives versioned reports that are never overwritten.** An engagement report for the principal, a short report for each person and a notice for urgent findings; each engagement report is filed with a fingerprint and the data behind it (Figure 12).
- **Safety matters stay with the person concerned.** Suspected covert monitoring by someone close is held in a restricted file that only two roles can open, and never reaches the engagement report (Figure 14).
- **Names stay out of every request to the AI assistant, and every action is logged.** Each request replaces every person by a reference (Figure 15); the audit log chains each entry to the one before (Figure 16).
- **The file is closed with a verified backup and a retention record.** The working folder is deleted only after the final backup has been decrypted successfully (Figure 17).

© Olivier BUSOLINI - 2026 - No reuse without permission

01
The household, person by person

The assessment starts with a register of people, because each person offers an attacker a different way in.

Staff who hold the principal's passwords or payments are assessed at the principal's tier.

A tier names the adversary to plan for, and so the protection each person needs.

A family is not one target. The principal, a spouse, a child and the staff who manage accounts or the residence each give an attacker a different route (unsourced). The Subject register records each of them with a reference, a type, a tier and a consent record, and states the rule it applies: "A subject's tier follows access, not status" (Subject register page, VIP app 1.0.1).

In the Haddad household the principal, Karim Haddad, is at T4, the highest of four tiers, because of an arbitration with a former partner, recorded as a step-up trigger (Triage and tiers page, VIP app 1.0.1). His executive assistant, Samir Khoury, is at T4 too; the register gives the reason as "delegated access: principal's tier". His spouse and daughter are at T3, "principal's tier minus one" (Figure 1).

FIGURE 1 · SUBJECT REGISTER OF THE HADDAD HOUSEHOLD

Ref	Label	Type	Relationship	Tier	Why	Interview consent	Checks consented
S1	Karim Haddad	Principal	principal	T4	set by the assessor; step-up trigger: dispute	yes	C1, C2, C6, C7, C8, C9
S2	Layla Haddad	Household adult	spouse	T3	principal's tier minus one	yes	—
S3	Nour Haddad	Minor	daughter	T3	principal's tier minus one	yes	C11
S4	Samir Khoury	Key staff	executive assistant	T4	delegated access: principal's tier	yes	C1, C2, C10
S5	Maria Santos	Key staff	house manager	T3	residence or routine access: principal's tier minus one	yes	—

Source: VIP app 1.0.1, Subjects page. Haddad Household (fictitious), test data, 26 September 2026.

The tier decides what protection is expected. The Triage and tiers page carries the framework's table: at T1 Private the adversary is "Opportunistic criminals: scams, mass phishing, commodity malware" and the expected minimum is "Baseline across all risks"; at T4 Strategic the adversary is "State actors and commercial spyware" and the minimum is "Hardened across all risks" (Triage and tiers page, VIP app 1.0.1).

FIGURE 2 · RESULTING TIERS, WITH THE REASON FOR EACH

Resulting tiers

Subject	Tier	Why
S1 Karim Haddad	T4	set by the assessor; step-up trigger: dispute
S2 Layla Haddad	T3	principal's tier minus one
S3 Nour Haddad	T3	principal's tier minus one
S4 Samir Khoury	T4	delegated access: principal's tier
S5 Maria Santos	T3	residence or routine access: principal's tier minus one

Source: VIP app 1.0.1, Triage and tiers page. Haddad Household (fictitious), test data, 26 September 2026.

Children take part through a parent or guardian. The register page says so where the consultant works: "Children are assessed through a parent or guardian only; never question a child" (Subject register page, VIP app 1.0.1).

© Olivier BUSOLINI - 2026 - No reuse without permission

02
Interviews, drafted answers and checks

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

Each adult is interviewed alone; a child's questions go to a parent.

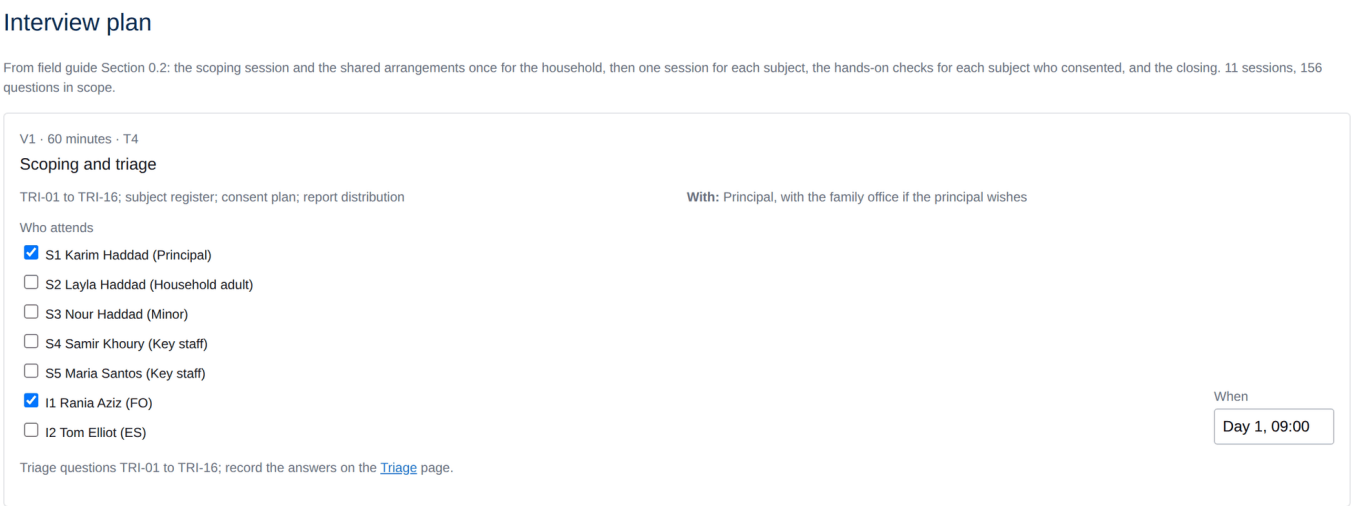
A drafted answer carries no weight until the consultant accepts it.

A level stated in interview is discounted until a check confirms it.

The interview plan is built from the register: "the scoping session and the shared arrangements once for the household, then one session for each subject, the hands-on checks for each subject who consented, and the closing". For the Haddads that comes to "11 sessions, 156 questions in scope" (Figure 3).

With consent, a session can be recorded and sent to AssemblyAI, a transcription service: the app "files a recording (through AssemblyAI) or a Teams or Zoom transcript against a session" (README.md, VI-PDLP repository). Claude, the AI assistant, then drafts one answer per question from the transcript, quoting the speaker, and the consultant accepts, edits or rejects each draft. The page is explicit: "Nothing is scored until you accept it" (Answers extracted page, VIP app 1.0.1).

FIGURE 3 · INTERVIEW PLAN: THE FIRST OF ELEVEN SESSIONS

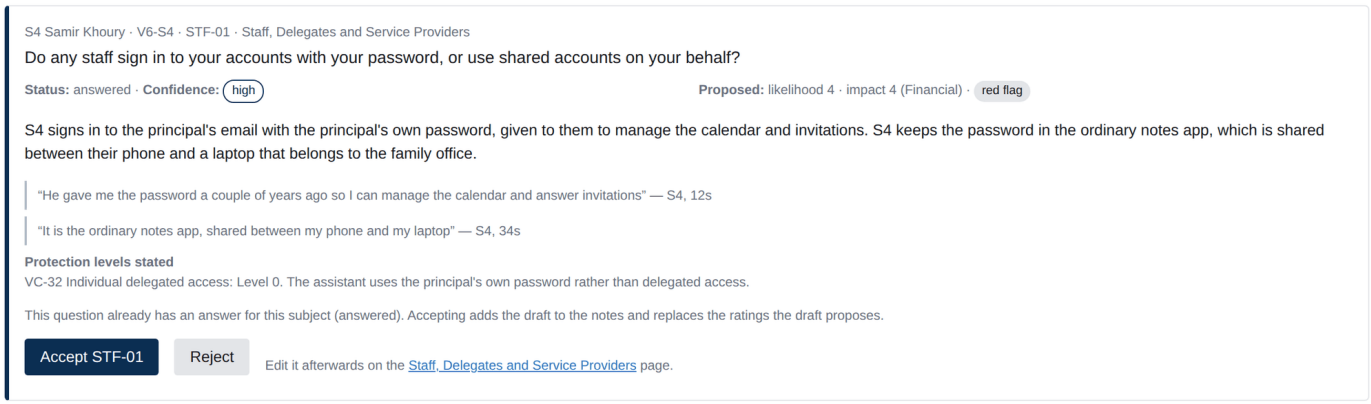


Source: VIP app 1.0.1, Interviews page. Haddad Household (fictitious), test data, 26 September 2026.

Figure 4 shows the draft for the executive assistant's answer on shared passwords. It quotes him twice, each quote with its time in the recording, proposes a likelihood of 4 and an impact of 4 on the financial dimension, and raises a red flag. The app checks every quote against the transcript: "Every draft quotes the transcript; the import refuses a response whose quotes are not in it" (Answers extracted page, VIP app 1.0.1).

© Olivier BUSOLINI - 2026 - No reuse without permission

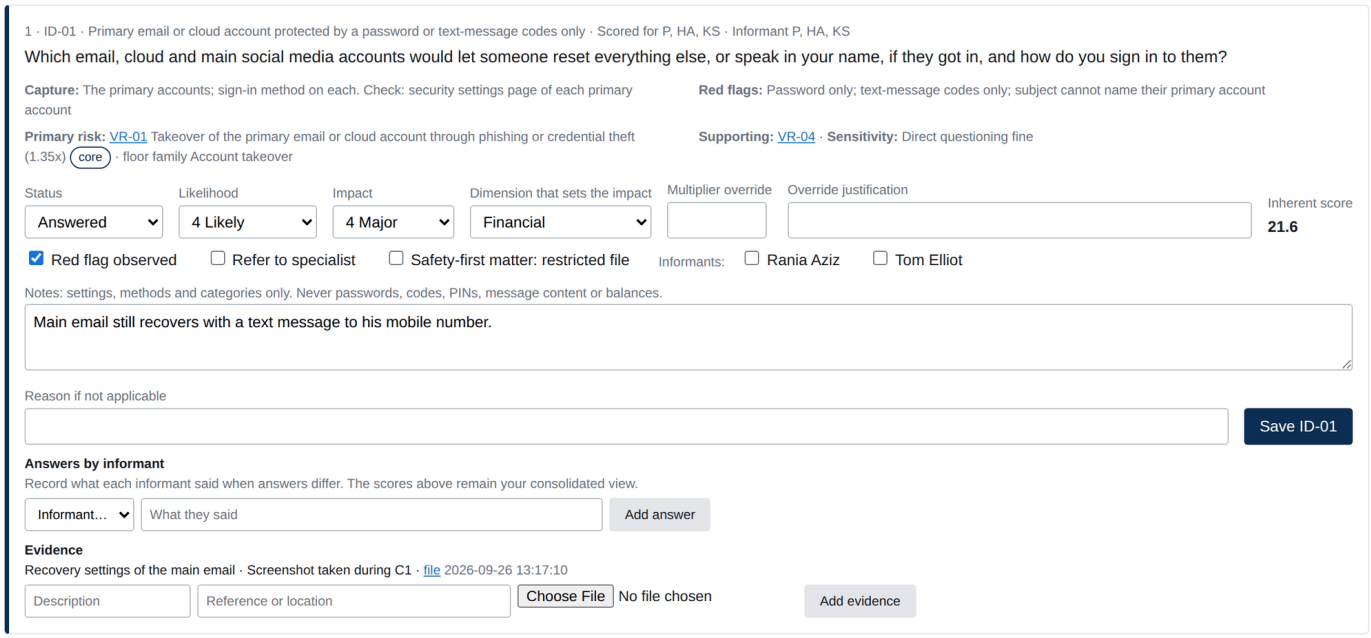
FIGURE 4 · A DRAFTED ANSWER, QUOTED FROM THE TRANSCRIPT, WAITING FOR REVIEW



Source: VIP app 1.0.1, Answers extracted page. Haddad Household (fictitious), test data, 26 September 2026.

Each question has its own entry: what to capture, what to check, the red flags, the risk it feeds and the scores (Figure 5). The Fieldwork page shows progress across the household, module by module and person by person, with the red flags counted (Figure 6).

FIGURE 5 · ONE QUESTION FOR THE PRINCIPAL: ID-01, THE PRIMARY EMAIL ACCOUNT



Source: VIP app 1.0.1, Identity and Accounts page. Haddad Household (fictitious), test data, 26 September 2026.

© Olivier BUSOLINI - 2026 - No reuse without permission

FIGURE 6 · FIELDWORK PROGRESS BY MODULE AND BY PERSON

Module	S1 Karim Haddad Principal · T4	S2 Layla Haddad Household adult · T3	S3 Nour Haddad Minor · T3	S4 Samir Khoury Key staff · T4	S5 Maria Santos Key staff · T3
Identity and Accounts	6 / 6 1 flag	6 / 6	—	6 / 6	6 / 6
Phones and Computers	6 / 7	6 / 6 1 flag	—	6 / 7	6 / 7
Messaging and Calls	4 / 4	3 / 3	—	4 / 4	4 / 4
Phone Number and Carrier	3 / 3	1 / 1	—	1 / 1	1 / 1
Cloud Data and Recovery	4 / 4	3 / 4	—	4 / 4	4 / 4
Exposure of Personal Data	5 / 5	6 / 6	3 / 3	3 / 3	3 / 3
Impersonation and Payments	4 / 4 1 flag	3 / 3	1 / 1	2 / 2 1 flag	2 / 2
Household and Family	—	2 / 2	1 / 1	—	—
Children (Parent-Led)	—	—	3 / 3	—	—
Staff, Delegates and Service Providers	1 / 1	—	—	4 / 4 1 flag	4 / 4
Home Network and Connected Devices	3 / 3	—	—	—	—
Travel	3 / 3	—	—	3 / 3	—
Detection, Response and Continuity	5 / 6	2 / 2	—	2 / 2	2 / 2

Source: VIP app 1.0.1, Fieldwork page. Haddad Household (fictitious), test data, 26 September 2026.

A protection level the family describes is recorded as Stated, and the app's rule is that it "counts one level lower, never below 0" (content/rules.json, VIP app 1.0.1, citing Framework v4 Sections 4.8 and 8). A hands-on check lets it count in full, and the check comes after consent: "A check needs the written consent recorded in the subject register first" (Checks page, VIP app 1.0.1).

© Olivier BUSOLINI - 2026 - No reuse without permission

03
What the assessment finds

One register for the household, scored per person, with the urgent findings raised first.

Protection in place cuts a risk score by up to 85%, and only the weakest control counts.

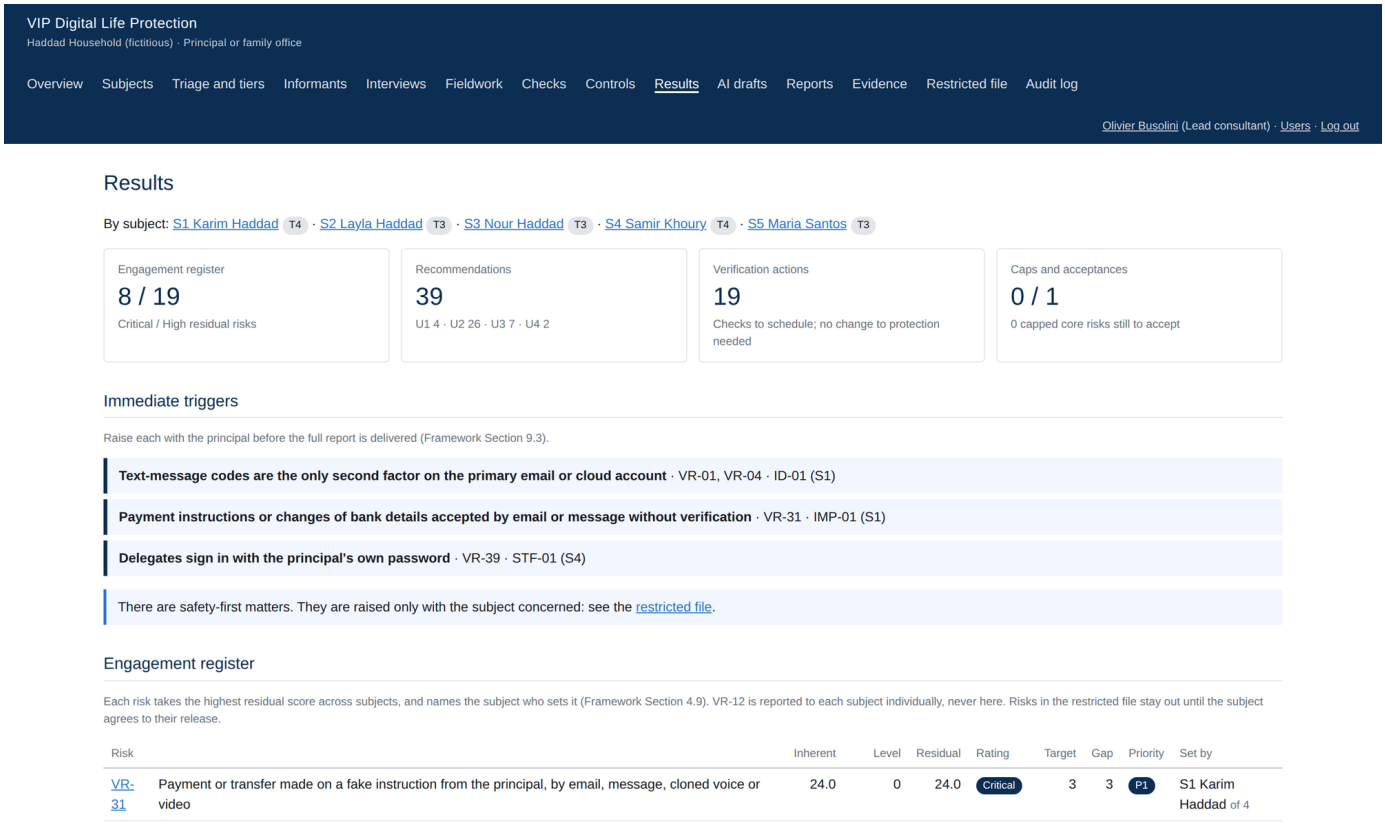
The register names the one person who sets each risk's score.

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

Each answer is scored for likelihood and impact, and the protection in place reduces the score. The app reduces the score by 40%, 65% and 85% at Levels 1, 2 and 3, and takes the risk's level as the "lowest counted level among the controls mapped to the risk" (content/rules.json, VIP app 1.0.1, citing Framework v4 Sections 4.1 to 4.9).

The Results page opens on four counts (Figure 7). For the Haddads: "8 / 19" Critical and High residual risks, 39 recommendations, 19 verification actions, and three immediate triggers to "Raise each with the principal before the full report is delivered (Framework Section 9.3)".

FIGURE 7 · RESULTS: THE COUNTS AND THE IMMEDIATE TRIGGERS



Source: VIP app 1.0.1, Results page. Haddad Household (fictitious), test data, 26 September 2026.

The engagement register lists each risk once: "Each risk takes the highest residual score across subjects, and names the subject who sets it (Framework Section 4.9)" (Figure 8). The first row is a payment or transfer made on a fake instruction from the principal, "by email, message, cloned voice or video", at 24.0, Critical, set by Karim Haddad.

© Olivier BUSOLINI - 2026 - No reuse without permission

FIGURE 8 · ENGAGEMENT REGISTER, FIRST ROWS

Engagement register

Each risk takes the highest residual score across subjects, and names the subject who sets it (Framework Section 4.9). VR-12 is reported to each subject individually, never here. Risks in the restricted file stay out until the subject agrees to their release.

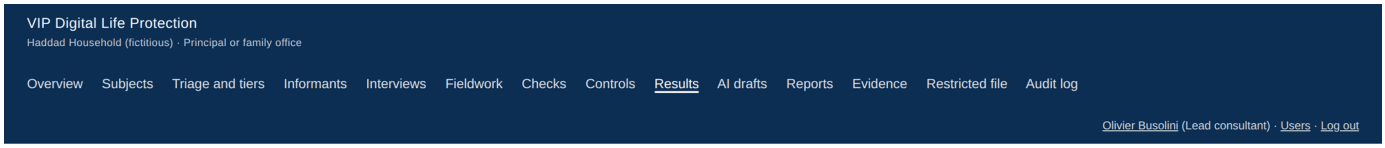
Risk		Inherent	Level	Residual	Rating	Target	Gap	Priority	Set by
VR-31	Payment or transfer made on a fake instruction from the principal, by email, message, cloned voice or video	24.0	0	24.0	Critical	3	3	P1	S1 Karim Haddad of 4
VR-42	Staff revealing the principal's schedule, location or residence through their own devices or social media core	22.4	0 (1 stated)	22.4	Critical	3	3	P1	S5 Maria Santos of 2
VR-02	Account recovery hijacked: recovery email, phone number or security answers controlled or guessable by an attacker core	21.6	0	21.6	Critical	3	3	P1	S1 Karim Haddad of 4
VR-18	SIM swap or unauthorised port-out of the principal's number core	21.6	0	21.6	Critical	3	3	P1	S1 Karim Haddad of 4
VR-25	Home address, residences and property ownership traceable through data brokers and public records core	21.6	0	21.6	Critical	3	3	P1	S2 Layla Haddad of 3
VR-28	Wealth, holdings or digital assets publicly linked to the principal core	21.6	0	21.6	Critical	3	3	P1	S1 Karim Haddad of 2
VR-14	Messaging account hijacked, or a linked device added without the owner noticing	20.8	0	20.8	Critical	3	3	P1	S4 Samir Khoury of 4
VR-21	Cloud backups and photos readable by anyone who takes over the account, for lack of end-to-end encryption	20.8	0 (1 stated)	20.8	Critical	2	2	P1	S2 Layla Haddad of 4
VR-19	Personal number widely known and used as an account identifier	19.2	0	19.2	High	3	3	P1	S1 Karim Haddad
VR-27	Personal data in breach dumps enabling targeting	19.2	0	19.2	High	3	3	P1	S4 Samir Khoury of 4
VR-35	Fake security or threat notifications used to phish the principal	19.2	0	19.2	High	3	3	P1	S1 Karim Haddad
VR-07	Targeted compromise of a phone by commercial spyware, including zero-click delivery core	18.0	0	18.0	High	3	3	P1	S1 Karim Haddad of 4

Source: VIP app 1.0.1, Results page. Haddad Household (fictitious), test data, 26 September 2026.

Each person also has their own view: their risks, the controls that limit each one, the residual and the priority. Figure 9 shows the principal's.

© Olivier BUSOLINI - 2026 - No reuse without permission

FIGURE 9 · THE PRINCIPAL'S OWN RESULTS



Results › S1 Karim Haddad

Karim Haddad

Principal · T4 (set by the assessor; step-up trigger: dispute) · core risks at or above target: 7%

Risks

Risk		Inherent	Controls	Level	Residual	Rating	Target	Gap	Priority	
VR-31	Payment or transfer made on a fake instruction from the principal, by email, message, cloned voice or video	24.0	VC-25, VC-26	0	24.0	Critical	3	3	P1	
VR-02	Account recovery hijacked: recovery email, phone number or security answers controlled or guessable by an attacker core	21.6	VC-03	0	21.6	Critical	3	3	P1	
VR-18	SIM swap or unauthorised port-out of the principal's number core	21.6	VC-03, VC-15, VC-16	0	21.6	Critical	3	3	P1	accepted
VR-28	Wealth, holdings or digital assets publicly linked to the principal core	21.6	VC-20, VC-22	0	21.6	Critical	3	3	P1	
VR-19	Personal number widely known and used as an account identifier	19.2	VC-03, VC-16	0	19.2	High	3	3	P1	
VR-35	Fake security or threat notifications used to phish the principal	19.2	VC-01, VC-28	0	19.2	High	3	3	P1	
VR-07	Targeted compromise of a phone by commercial spyware, including zero-click delivery core	18.0	VC-08, VC-09, VC-11	0	18.0	High	3	3	P1	
VR-08	Malware or unwanted remote-access software on personal or family devices	15.6	VC-06, VC-09	0	15.6	High	3	3	P1	
VR-17	Malicious links, attachments or files received from unknown contacts	15.6	VC-08, VC-28	0	15.6	High	3	3	P1	

Source: VIP app 1.0.1, Results for S1 page. Haddad Household (fictitious), test data, 26 September 2026.

© Olivier BUSOLINI - 2026 - No reuse without permission

04

What to do, and in what order

Each recommendation offers three levels of protection, the risk left at each, and what it costs in daily life.

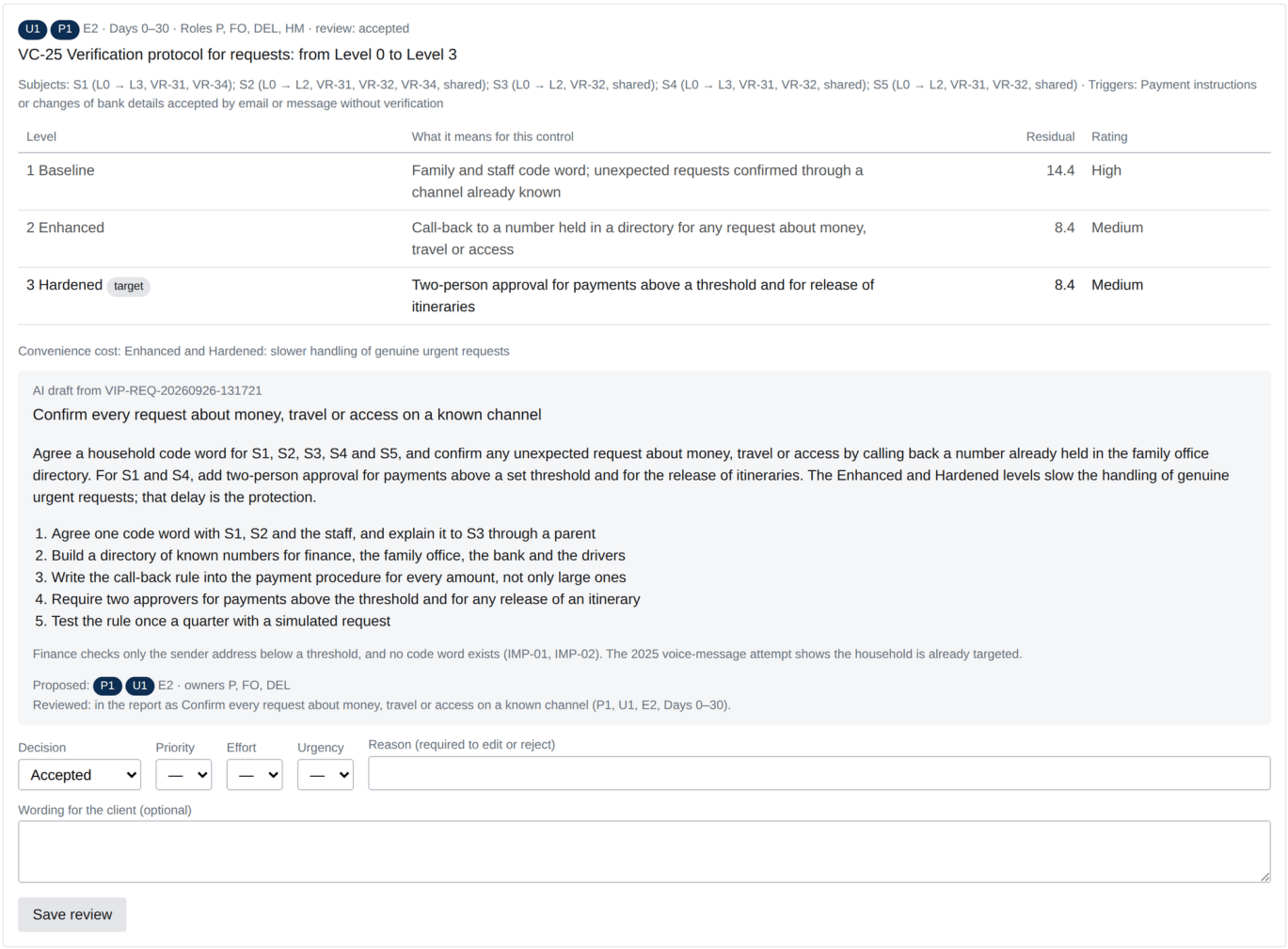
The family sees the protection gained and the convenience lost before it decides.

The most urgent actions start within 7 days.

A recommendation names the control, the people it serves and three levels: Baseline, Enhanced and Hardened. For each level it gives the residual score and rating, and it names the convenience cost. For the verification of requests, a code word at Baseline leaves the payment risk at 14.4, High; a call-back to a number held in a directory, at Enhanced, brings it to 8.4, Medium. The cost is stated as "slower handling of genuine urgent requests" (Figure 10).

The consultant reviews every recommendation before it reaches a report. Where Claude drafted the client wording, the draft sits beside the calculation, and the review is recorded against that draft (Figure 10).

FIGURE 10 · A RECOMMENDATION WITH ITS THREE LEVELS AND THE REVIEWED WORDING



Source: VIP app 1.0.1, Results page. Haddad Household (fictitious), test data, 26 September 2026.

The 30/60/90-day roadmap places each action by urgency, from U1, the most urgent, to U4. In the test household thirty actions fall in the first 30 days. The five marked U1 are phone hardening mode for four people, confirmation of every request about money, travel

© Olivier BUSOLINI - 2026 - No reuse without permission

or access on a known channel, a password manager with separate vaults, delegated access for the assistant and the house manager in place of the principal's password, and a review of connected apps, forwarding rules and active sessions (Figure 11). The app's rules give a U1 action a start within 7 days (content/rules.json, VIP app 1.0.1, citing Framework v4 Section 9.3).

FIGURE 11 · 30/60/90-DAY ROADMAP

30/60/90-day roadmap

Window	Recommendations
Days 0–30	VC-08 Turn on the phone hardening mode for S1, S2, S4 and S5 (U1); VC-25 Confirm every request about money, travel or access on a known channel (U1); VC-02 Move the household and staff to a password manager with separate vaults (U1); VC-32 Give S4 and S5 their own delegated access instead of the principal's password (U1); VC-01 Put security keys on the primary accounts of S3 and S4 (U2); VC-03 Take the phone number out of account recovery (U2); VC-05 Review of connected apps, forwarding rules and active sessions (U1); VC-06 Updates and replacement of unsupported devices (U2); VC-09 Compromise checks, including for spyware (U2); VC-11 Separation of corporate and personal devices (U2); VC-12 End-to-end encrypted messaging with account locks (U2); VC-13 Message retention rules (U2); VC-14 Discipline for sensitive conversations (U2); VC-16 Separation of phone numbers (U2); VC-17 End-to-end encrypted cloud storage (U2); VC-20 Personal data removal and monitoring (U2); VC-21 Discipline on location and routines (U2); VC-22 Management of the public profile and wealth disclosure (U2); VC-23 Monitoring of breach exposure (U2); VC-24 Footprint of family and staff (U2); VC-28 Briefing on social engineering (U2); VC-29 Protection of children's accounts and devices (U2); VC-34 Staff vetting and confidentiality (U2); VC-39 Travel device regime (U2); VC-40 Assessment before travel (U2); VC-41 Alerting on signs of compromise (U2); VC-15 Carrier account protection (U2); VC-27 Monitoring and takedown of impersonation (U2); VC-33 Staff joining and leaving (U2); VC-42 Incident response plan and contracted responder (U2)
Days 31–60	VC-04 Account inventory and clean-up of legacy accounts (U3); VC-07 Device lock, theft protection and accessory control (U3); VC-18 Custody of recovery material (U3); VC-19 Controlled sharing of sensitive documents (U3); VC-31 Separation on shared household devices and accounts (U3); VC-35 Due diligence and access limits for service providers (U3); VC-36 Home network separation (U3)
Days 61–90	VC-37 Security of connected devices (U4)
Beyond 90 days	—

Source: VIP app 1.0.1, Results page. Haddad Household (fictitious), test data, 26 September 2026.

© Olivier BUSOLINI - 2026 - No reuse without permission

05

What the family receives

An engagement report for the principal, a short report for each person, and a notice for what cannot wait.

Each engagement report is kept as issued, with its fingerprint and its data.

The next assessment shows what moved since the last report.

The Reports page names what the family receives: "the engagement report for the principal, a short report for each subject, and the immediate attention notice. Each file is saved unchanged in the client's reports folder, with a data snapshot beside it" (Figure 12).

The Haddad engagement report runs to 44 pages at version 1.2 and carries 38 recommendations; the consultant rejected one of the 39 in review. "Drafts are numbered 0.1, 0.2 before the first final report, and finals 1.0, 2.0. A report is never overwritten"; a draft made after a final takes the next point, as 1.1 and 1.2 show (Figure 12).

© Olivier BUSOLINI - 2026 - No reuse without permission

FIGURE 12 · REPORTS: ENGAGEMENT REPORT VERSIONS AND THE REPORTS FOR EACH PERSON

Reports

Three documents, in the Olivier Busolini document style: the engagement report for the principal, a short report for each subject, and the immediate attention notice. Each file is saved unchanged in the client's reports folder, with a data snapshot beside it.

Engagement report

For the principal. Reassessment: compare with a previous engagement report. It carries only accepted and edited recommendations, and nothing from the restricted file: matters under the safety-first protocol go only into the report of the person concerned. A baseline is set, so the report includes a section on what changed since version 1.0 (Reassessment).

All checks pass. 38 recommendation(s) will be included.

2 deferred question(s) will be listed as open points.

(•) Draft (marked as draft; can be produced at any time) ( ) Final (every check must pass; lead consultant only)

[Create engagement report]

Drafts are numbered 0.1, 0.2 before the first final report, and finals 1.0, 2.0. A report is never overwritten.

Version	Status	Created	Pages	Recommendations	Fingerprint (SHA-256)	
1.2	draft	2026-09-26 13:17:30	44	38	1743a0baaf95c37e…	PDF · Data
1.1	draft	2026-09-26 13:17:14	43	38	9ac67bec872c2c96…	PDF · Data
1.0	final	2026-09-26 13:17:12	41	38	fca2f04a4b4ab6e4…	PDF · Data
0.1	draft	2026-09-26 13:17:11	41	38	98ef23a9531912bb…	PDF · Data

Reports for each subject

A short report for one person: their own risks and actions. A child's report is addressed to the parent or guardian. A report you produce includes the person's restricted matters where there are any; it is then filed apart, and only the lead consultant and the reviewer can open it. Earlier reports of a person are withdrawn to the same place when a matter of theirs enters the restricted file.

Subject	Type	
S1 Karim Haddad	Principal	[Create report]
S2 Layla Haddad	Household adult	[Create report]
S3 Nour Haddad	Minor	[Create report]
S4 Samir Khoury	Key staff	[Create report]
S5 Maria Santos	Key staff	[Create report]

Filed: S5_individual_report_20260926_131714_2a12.pdf · S4_individual_report_20260926_131714_12b1.pdf · S3_individual_report_20260926_131732_2635.pdf · S3_individual_report_20260926_131714_860f.pdf · S1_individual_report_20260926_131731_9f33.pdf · S1_individual_report_20260926_131713_ef06.pdf

Immediate attention notice

Source: VIP app 1.0.1, Reports page. Haddad Household (fictitious), test data, 26 September 2026.

A later engagement compares against any earlier report. Set against version 1.0, the test household shows "1 risk(s) improved, 0 slipped, 50 unchanged" and "2 protection level(s) higher, 0 lower" (Figure 13). The framework sets the rhythm: "annually, every six months at T4, and after any step-up trigger or incident" (Reassessment page, VIP app 1.0.1, citing Framework v4 Section 5).

© Olivier BUSOLINI - 2026 - No reuse without permission

FIGURE 13 · REASSESSMENT AGAINST REPORT 1.0

Reassessment

Compare this engagement with a previous one for the same household (Framework v4 Section 5: annually, every six months at T4, and after any step-up trigger or incident). The baseline is the data snapshot saved beside any engagement report; one from a previous engagement can be uploaded from its folder or a restored backup. Setting it changes nothing in the scores: the next engagement report gains a section on what moved.

An engagement report snapshot from this folder

Choose…

or a snapshot from elsewhere

Choose File No file chosen

Set as baseline

Since version 1.0 of 2026-09-26

1 risk(s) improved, 0 slipped, 50 unchanged, 0 new, 0 no longer scored. 2 protection level(s) higher, 0 lower. Of 37 recommendation(s) made then: 0 met, 2 progressed, 35 not acted on, 0 worse.

What happened to the last recommendations

Control	Then	Now	Lowest level	Outcome
VC-03 Account recovery hardening: Level 3	P1	P1	0 → 0	untouched
VC-06 Updates and replacement of unsupported devices: Level 3	P1	P1	0 → 0	untouched
VC-08 Platform hardening mode: Level 3	P1	P1	0 → 0	untouched
VC-11 Separation of corporate and personal devices: Level 3	P1	P1	0 → 0	untouched
VC-12 End-to-end encrypted messaging with account locks: Level 3	P1	P1	0 → 0	untouched
VC-13 Message retention rules: Level 3	P1	P1	0 → 0	untouched
VC-14 Discipline for sensitive conversations: Level 3	P1	P1	0 → 0	untouched
VC-16 Separation of phone numbers: Level 3	P1	P1	0 → 0	untouched
VC-17 End-to-end encrypted cloud storage: Level 3	P1	P1	0 → 0	untouched
VC-20 Personal data removal and monitoring: Level 3	P1	P1	0 → 0	untouched
VC-21 Discipline on location and routines: Level 3	P1	P1	0 → 0	untouched
VC-22 Management of the public profile and wealth disclosure: Level 3	P1	P1	0 → 0	untouched

Source: VIP app 1.0.1, Reassessment page. Haddad Household (fictitious), test data, 26 September 2026.

© Olivier BUSOLINI - 2026 - No reuse without permission

06

How the family's material is protected

Safety matters stay with the person concerned, and every action on the file is logged.

Suspected monitoring by someone close is raised only with the person concerned.

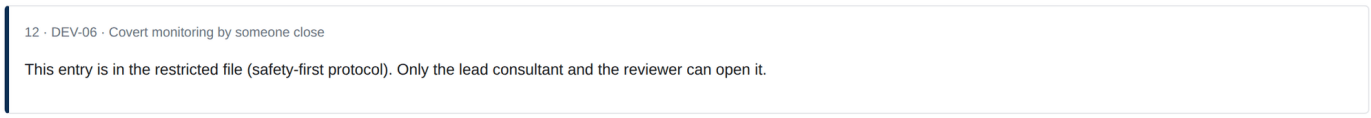
Names never go to the AI assistant; references do.

Nothing is deleted before the final backup has been shown to open.

Some findings cannot be handled like the others. The Restricted file page sets the rule: "Safety-first matters (field guide Section 1): suspected covert monitoring, or a threat from someone close to a subject. Open to the lead consultant and the reviewer only. Report only to the subject concerned, through a channel they choose, never to a suspected person" (Restricted file page, VIP app 1.0.1).

The engagement report "carries only accepted and edited recommendations, and nothing from the restricted file" (Reports page, VIP app 1.0.1). A consultant without that access sees only that an entry exists (Figure 14).

FIGURE 14 · A RESTRICTED ENTRY, AS A CONSULTANT SEES IT

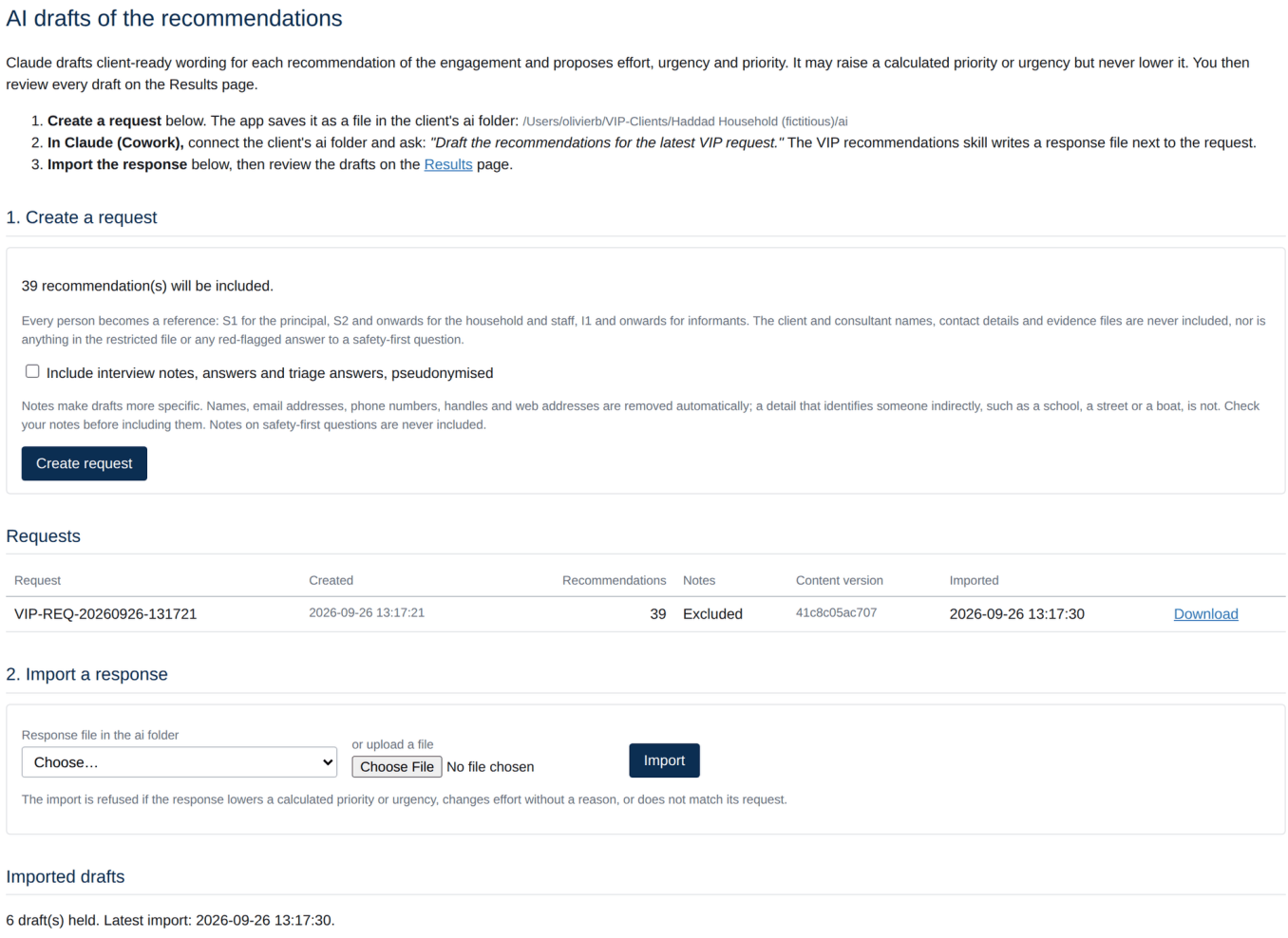


Source: VIP app 1.0.1, Phones and Computers page, signed in as a consultant. Haddad Household (fictitious), test data, 26 September 2026.

Claude drafts wording from a request file that the consultant creates and reads first. The page states what goes into it: "Every person becomes a reference: S1 for the principal, S2 and onwards for the household and staff, I1 and onwards for informants. The client and consultant names, contact details and evidence files are never included, nor is anything in the restricted file or any red-flagged answer to a safety-first question" (Figure 15).

© Olivier BUSOLINI - 2026 - No reuse without permission

FIGURE 15 · AI DRAFTS: THE REQUEST, WHAT IT CONTAINS, AND THE IMPORT CHECKS

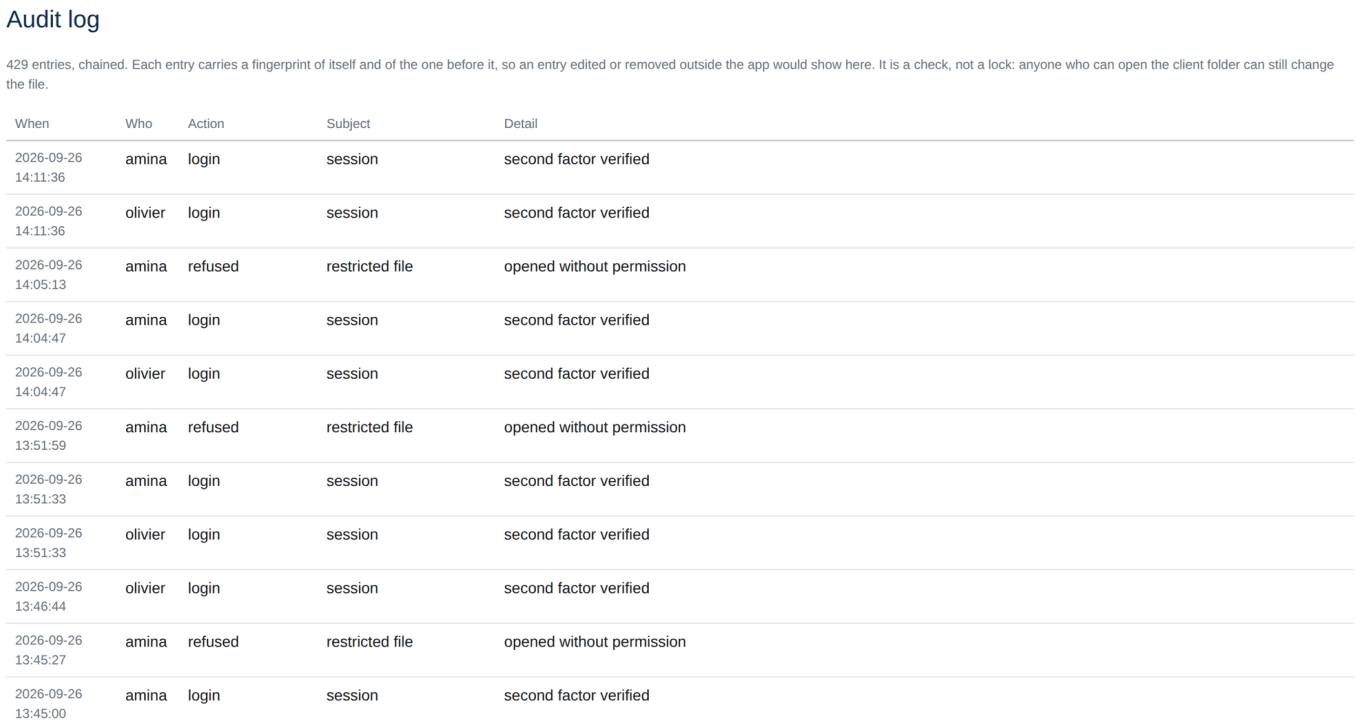


Source: VIP app 1.0.1, AI drafts page. Haddad Household (fictitious), test data, 26 September 2026.

"Every user signs in with a password of 12 characters or more and a code from an authenticator app" (VIP app - User guide 1.0.0, Executive summary), and every action is recorded. The audit log states 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" (Figure 16). The refusals in the log are the test consultant account being turned away from the restricted file.

© Olivier BUSOLINI - 2026 - No reuse without permission

FIGURE 16 · AUDIT LOG, MOST RECENT ENTRIES



Audit log

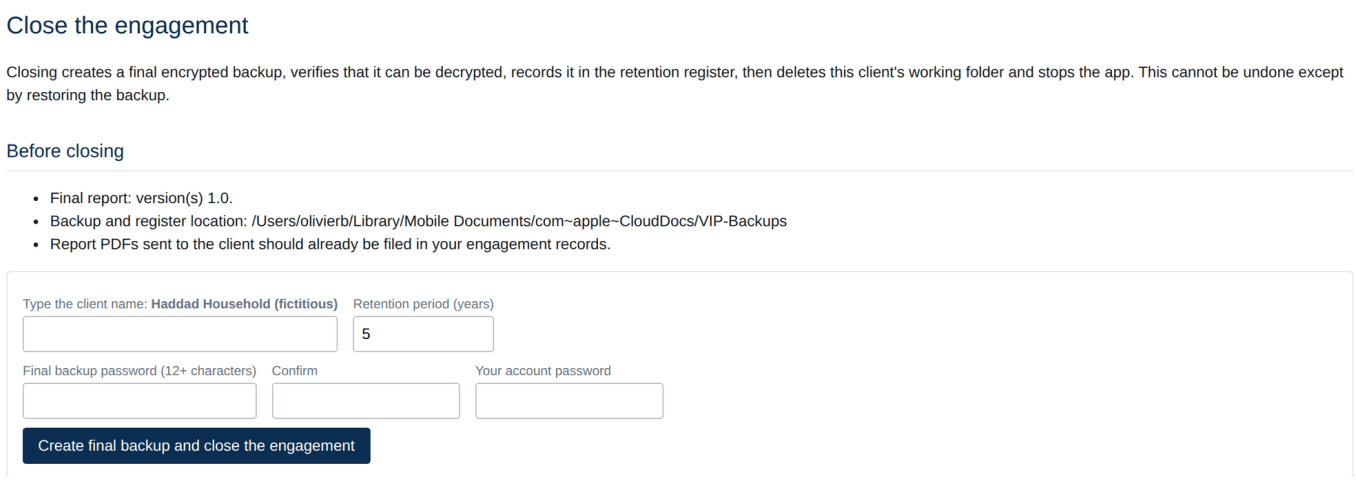
429 entries, chained. Each entry carries a fingerprint of itself and of the one before it, so an entry edited or removed outside the app would show here. It is a check, not a lock: anyone who can open the client folder can still change the file.

When	Who	Action	Subject	Detail
2026-09-26 14:11:36	amina	login	session	second factor verified
2026-09-26 14:11:36	olivier	login	session	second factor verified
2026-09-26 14:05:13	amina	refused	restricted file	opened without permission
2026-09-26 14:04:47	amina	login	session	second factor verified
2026-09-26 14:04:47	olivier	login	session	second factor verified
2026-09-26 13:51:59	amina	refused	restricted file	opened without permission
2026-09-26 13:51:33	amina	login	session	second factor verified
2026-09-26 13:51:33	olivier	login	session	second factor verified
2026-09-26 13:46:44	olivier	login	session	second factor verified
2026-09-26 13:45:27	amina	refused	restricted file	opened without permission
2026-09-26 13:45:00	amina	login	session	second factor verified

Source: VIP app 1.0.1, Audit log page. Haddad Household (fictitious), test data, 26 September 2026.

At the end of the engagement the lead consultant closes the file: "Closing creates a final encrypted backup, verifies that it can be decrypted, records it in the retention register, then deletes this client's working folder and stops the app" (Figure 17).

FIGURE 17 · CLOSING THE ENGAGEMENT



Close the engagement

Closing creates a final encrypted backup, verifies that it can be decrypted, records it in the retention register, then deletes this client's working folder and stops the app. This cannot be undone except by restoring the backup.

Before closing

- Final report: version(s) 1.0.
- Backup and register location: /Users/olivierb/Library/Mobile Documents/com~apple~CloudDocs/VIP-Backups
- Report PDFs sent to the client should already be filed in your engagement records.

Type the client name: **Haddad Household (fictitious)**

Retention period (years) 5

Final backup password (12+ characters)

Confirm

Your account password

Create final backup and close the engagement

Source: VIP app 1.0.1, Close the engagement page. Haddad Household (fictitious), test data, 26 September 2026.

© Olivier BUSOLINI - 2026 - No reuse without permission

07
Sources

The documents and pages this one draws on.

1 VIP digital life protection framework v4 (available on request)

2 VIP digital life protection fieldwork questionnaire v1 (available on request)

3 VIP digital life protection field guide v1 (available on request)

4 VIP app 1.0.1: screens of the Haddad Household (fictitious), captured 26 September 2026

5 VIP app 1.0.1: rules file (content/rules.json) and README

6 VIP app - User guide 1.0.0

© 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	Subjects	Each person, with type, tier, reason and consent
Figure 2	Triage and tiers	The tier each person receives, and why
Figure 3	Interviews	The interview plan, session by session
Figure 4	Answers extracted	A drafted answer with its quotes, before review
Figure 5	Identity and Accounts	One question: guidance, scores and evidence
Figure 6	Fieldwork	Progress by module and person, with red flags
Figure 7	Results	Counts and immediate triggers
Figure 8	Results	The engagement register
Figure 9	Results for S1	The principal's risks and controls
Figure 10	Results	A recommendation with three levels and its reviewed wording
Figure 11	Results	The 30/60/90-day roadmap
Figure 12	Reports	Report versions and personal reports
Figure 13	Reassessment	What changed since report 1.0
Figure 14	Phones and Computers	The restricted entry, consultant view
Figure 15	AI drafts	The pseudonymised request and the import checks
Figure 16	Audit log	The chained record of actions
Figure 17	Close the engagement	Final backup, verification and retention

Source: VIP app 1.0.1. Haddad Household (fictitious), test data, 26 September 2026.

© Olivier BUSOLINI - 2026 - No reuse without permission

Appendix B: How this tour was prepared

The household is fictitious. The Overview page of the test folder records its scope as "Fictitious household for testing the VIP app. No real person, answer or finding." The names, the arbitration, the 2025 voice-message attempt and every answer were invented for testing.

The folder was prepared with the app's own tool, tools/prep_test_client.py with the full stage, which enters every answer, level, check, review and report through the app's pages. A 12-turn fictitious transcript for the executive assistant was then added, with an answer extraction and a set of AI drafts written for the test, so that every page carries content.

The screens were captured on VIP app 1.0.1 on 26 September 2026, in Chromium at a width of 1,440 pixels and twice the usual pixel density, signed in as the lead consultant or, where marked, as a consultant. Each figure is a region of one page, cut at a row or block boundary; the page footer, which carries the version and the data folder, is hidden. On the Reports page the line that lists reports filed in the restricted file is hidden as well, so the tour points at no fictitious person's safety matter.

Figures quoted in the text are read from the screens shown or from the app's rules file, content/rules.json, which names the framework section each rule applies. One general statement, in Section 01, rests on no source and is marked unsourced.

© Olivier BUSOLINI - 2026 - No reuse without permission