SAMPLE DELIVERABLE

EXTERNAL SECURITY REVIEW — METHODOLOGY SAMPLE

This is a sanitized template based on real client work, shown here to illustrate how we structure, prioritize, and source a passive external security review. Company names and identifying specifics have been replaced with placeholders.

SUBJECT	CATEGORY	PREPARED FOR	DATE
[Client Company]	[Client's Industry]	[Client] Leadership	[Date]

● VERIFIED confirmed by direct observation of the public site

○ INFERRED a reasonable read of what's visible

■ UNCONFIRMED needs a code-level or internal check

▲ SEC. 01

EXECUTIVE SUMMARY

- **This is a first-pass, passive read** of [Client]'s public marketing site only; no credentials, scanning, or active testing was performed against any system. ● VERIFIED
- **The core operating platform holds materially more sensitive data** than the marketing site does, and should be treated as its own, higher-priority engagement. ○ INFERRED
- **The marketing site is the lowest-risk part** of the footprint reviewed here. ○ INFERRED
- **Several findings need an internal or code-level check** to confirm; a passive external read can flag a pattern but can't verify what happens server-side. ■ UNCONFIRMED

▲ SEC. 02

SCOPE & METHODOLOGY

IN SCOPE

Public page content and structure; lead and contact forms (visible behavior only); linked pages and subdomains; data handling as described in the site's own copy.

OUT OF SCOPE (THIS PASS)

HTTPS/TLS configuration and certificate detail; security headers (CSP, HSTS, X-Frame-Options); CMS/platform version disclosure and admin-path exposure; server-side validation, authentication, and session handling.

This pass is a passive, external read: page content, structure, forms, and linked pages only. No credentials were used and no active probing, scanning, or testing was performed against any system. Treat it as a first orientation, not a substitute for a credentialed technical review.

▲ SEC. 03

KEY FINDINGS

FINDING 01 · VERIFIED

LEAD FORMS SHOW NO VISIBLE SPAM PROTECTION

No CAPTCHA, honeypot, or rate-limiting indicator is visible on the site's lead or contact forms. Forms without this protection are a common target for automated spam and, if inputs aren't sanitized server-side, a possible injection vector. Whether submissions are validated server-side isn't visible from outside and needs a code-level check.

FINDING 02 · VERIFIED

CONFIDENTIAL-DOCUMENT LANGUAGE LEFT ON PUBLIC PAGES

Public pages carry a footer restricting distribution "outside the recipient's organization," language that reads like boilerplate carried over from a confidential deck or PDF template and left on fully public, indexable pages. It isn't a technical vulnerability, but it's a real inconsistency: either the language should come off, or the pages should actually be access-restricted if it's meant literally.

FINDING 03 · INFERRED

THIRD-PARTY INTEGRATIONS WARRANT THEIR OWN REVIEW

Marketing copy describes a financial-software integration and an AI layer that can take plain-language commands and trigger real actions. Any integration that moves financial data, or lets an AI layer act on a live record, needs its own review of API scopes, token handling, and what it's allowed to do without a human confirming it first. The copy states outputs are reviewed before sending; that's a good pattern, worth verifying it's actually enforced in code and not only in the marketing description.

UNCONFIRMED

FINDING 04 · INFERRED

A SUBDOMAIN MAY NOT INHERIT THE MAIN SITE'S POSTURE

A separate subdomain hosts a distinct program and is frequently on different infrastructure with a different patch level. It's worth including explicitly in scope rather than assuming it inherits the main site's security posture.

FINDING 05 · UNCONFIRMED

THE PLATFORM, NOT THE WEBSITE, HOLDS THE REAL EXPOSURE

Site copy describes an onboarding flow, delivered via a tokenized link, that collects sensitive personal and financial information (illustrative examples: banking details for pay, government ID, licensing or certification records, employment history). This is the highest-value target in the footprint. Where and how this data is stored, whether it's encrypted at rest, and who can access it is the single most important thing to verify, and alone justifies a platform-level review as a priority rather than a nice-to-have.

Priority reframe: a marketing-site review is a reasonable first pass, but it isn't the audit that matters most. Any flow collecting banking details, government ID, or licensing records belongs in a dedicated, credentialed review before a public-facing pass is called complete.

▲ SEC. 04

RECOMMENDED NEXT STEPS

Run a baseline header/TLS scan

Free public tools (e.g. securityheaders.com, SSL Labs); no access needed for a baseline on transport security and header hygiene

Low

effort

Get read access to hosting/CMS admin or a code export

Enables a direct review of form handling, header config, and CMS hardening instead of external inference

Low

effort

Prioritize a review of the core operating platform

This is where PII, banking, and identity documents actually live; materially higher risk than the marketing site

High

effort

Remove or correct the confidentiality footer on public pages

Small credibility issue; either restrict the pages or drop the language

Low

effort

Confirm CAPTCHA/honeypot and server-side validation on lead forms

Closes a common spam and injection vector

Low

effort

▲ SEC. 05

OPEN VERIFICATION ITEMS

OPEN	Whether lead-form submissions are validated server-side; not visible from outside.
OPEN	Whether onboarding data is encrypted at rest, and precisely who has access to it.
OPEN	Whether the "reviewed before sending" claim for AI-driven actions is enforced in code, not only described in marketing copy.
OPEN	Patch level and security posture of secondary subdomains relative to the main site.

Sources — client's public marketing site, linked subdomains, and page copy describing platform behavior. Compiled [Date] · Passive, external pass only; not a substitute for a full security audit or penetration test.

This sample shows our approach to external security review: findings confidence-tagged and separated from what still needs verification, effort scoped honestly, and the real risk named plainly even when it sits outside this pass's scope. **Get in touch** to talk about a review like this for your team.