Dodu Security
Smart contract audits and pentests

Andrei Dodu
Sweden
andrei@dodu.se
dodu.se

Proposal and statement of work

This is the template. Each proposal replaces the bracketed fields and is sent as a PDF. Once signed it is the whole agreement: scope, price, dates and what happens if the scope moves.

1. PARTIES

[CLIENT LEGAL NAME], registered at [ADDRESS], [COUNTRY] (the Client) and Andrei Dodu, trading as Dodu Security, Sweden (the Auditor).

2. ENGAGEMENT

[One sentence: what is being reviewed and why. Example: a pre-launch security review of the vault, staking and reward contracts ahead of mainnet deployment.]

3. SCOPE

Reviewed at commit [COMMIT HASH] on [BRANCH/TAG]:

- [Repository and path]: [contract or module names]
- [Repository and path]: [contract or module names]
- [Integrations reviewed: oracle, DEX, bridge, access-control model]

4. OUT OF SCOPE

Not reviewed under this engagement, and quotable as an exclusion later:

- gas and transaction economics, and MEV beyond what the in-scope code creates;
- front-end, wallet and UX code;
- off-chain services, indexers, keepers and infrastructure, unless listed in section 3;
- legal, regulatory and tax questions;
- key custody beyond the ownership and permission checks named in scope;
- changes made after the commit above.

5. DELIVERABLES

- A severity-rated report in PDF and Markdown, with a runnable proof of concept for every High and Critical.
- A coverage statement naming the commit, the files read, the integrations covered and the exclusions.
- One fix-review round within 5 working days of the Client’s patches, with each finding marked fixed, partially fixed, acknowledged or not fixed.
- A 45-minute exit call with the Client’s engineers.

6. DATES

- Kickoff: [DATE], within 24 to 72 hours of the signed scope and repository access.
- Draft report: [DATE], [N] business days after kickoff.
- Final report: within 3 business days of receiving the Client’s responses.
- Fix review: within 5 business days of the patches landing.

7. FEE AND PAYMENT

[AMOUNT] USD, fixed for the scope above. Payable 50% on signature and 50% on delivery of the final report, by bank transfer or USDC to the address on the invoice. Invoiced in USD; if the Client needs another currency, the rate and the invoiced amount are agreed in writing before signature. Bank charges are the Client’s. Work outside the scope in section 3 is quoted separately and started only on written approval.

8. CLIENT RESPONSIBILITIES

Repository access at the commit above; an architecture note; known issues and prior audit reports; a named technical contact who answers within one working day; and the signed rules of engagement before testing starts. Delays in these shift the dates in section 6 by the same number of days.

9. CHANGE CONTROL

If the scope changes after signature (new contracts, a moved commit, a different architecture), the Auditor states the effect on fee and dates in writing before doing the work. Nothing is added to the invoice that was not agreed in writing first.

10. CONFIDENTIALITY AND DISCLOSURE

The mutual NDA signed by the parties applies. Findings are disclosed to the Client only. Nothing is published without written consent, and no finding is published before the fix is deployed.

11. LIABILITY

The review is performed with reasonable skill and care and does not warrant that every vulnerability will be found. Liability is capped at the fee paid. Neither party is liable for indirect or consequential loss.

12. GOVERNING LAW

[Sweden / other], with the courts of [venue] having exclusive jurisdiction.

For the Client: name, title, date, signature

Signature

For Dodu Security: Andrei Dodu, date, signature

Signature

Dodu Security is the trading name of Andrei Dodu. This document is a template, not legal advice; where the engagement is large enough to warrant it, have a lawyer read it.