NTO-26040 · System Audit

An Independent Assessment of the System You Already Have

1. WHO THIS IS FOR

A company with a system built by someone else, or by a team that is no longer there, that needs to know its real state before deciding what to do with it: keep investing, rescue it, modernize it, migrate it, hand over its maintenance, or replace it.

2. WHAT'S INCLUDED

Fixed scope, fixed price. The limits below are what the price is built on: anything above them moves to the next tier or is quoted separately.

Tier	Repositories	Applications	Environments	Integrations	Approx. size
Focused	**1**	**1**	**Up to 2**	**Up to 2**	**Up to 25 screens**
Standard	**Up to 3**	**Up to 2**	**Up to 3**	**Up to 5**	**Up to 60 screens**
Extended	**Up to 6**	**Up to 4**	**Up to 4**	**Up to 10**	**Up to 120 screens**

Functionality included: code quality and maintainability, architecture and technical debt, security posture, performance and scalability, data model and data integrity, dependencies and licensing, infrastructure and deployment, test coverage, documentation and knowledge risk, operational risk, and an estimate of what it would take to fix what matters.

Every project includes design, development, QA and project management as required. Technology and architecture decisions are made by NTSprint Engineering at kick-off and written into the proposal.

How we count

Limit	What counts
What we audit	The system as it is today, from the source code, the running environments and a set of interviews. We do not modify anything.
Repositories	Each independent repository we are given access to. Monorepos with several applications count by application, not by repository.
Applications	Each independently deployable application: a web front end, an API, a background worker, a mobile app.
Environments	Each running environment we are given access to, for example production and staging.
Integrations	Each external system the product connects to. We review how the connection is built and where it can fail; we do not audit the third party's system.
Size	An approximate measure used to size the audit, not a hard limit. If the system turns out to be materially larger than declared, we say so within the first two days and agree the tier before continuing.
Independence	The audit is written to be read by someone who did not build the system. Findings are ranked by severity and business impact, not by technical preference.

3. DELIVERABLES, TIMELINE AND PRICE

Tier	Duration	Price
Focused	1 day	**$250**
Standard	2 days	**$300**
Extended	3 days	**$350**

Fixed price for the scope defined above. Not time and materials. Work beyond the stated boundary is quoted separately as a Change Request.

The timeline starts once we have the code, data, and access needed to begin, not at signature.

The full price of the audit is credited against any project you contract with us within 60 days of receiving the report. If you decide to work with someone else, or to do nothing, the report is yours to use.

What you receive

• Audit report, written to be read by a non-technical decision-maker	• Dependency and licensing inventory • Remediation roadmap with effort ranges per item

• Findings register, ranked by severity and business impact • Risk matrix: what can fail, how likely and what it would cost • Architecture and data model as they actually are today	• A clear recommendation: keep, rescue, modernize, migrate, hand over maintenance, or replace • A recorded live session to walk you through the findings and answer questions

How the work is delivered

Stage	What is working at the end of it
1. Access and inventory	Access granted, the system inventoried: repositories, applications, environments, dependencies and integrations mapped
2. Analysis	Tool-assisted and manual review of code, architecture, security, data, performance, tests and deployment
3. Interviews and validation	Findings checked against how the system is actually used and operated, with the people who run it
4. Report and recommendation	The written report delivered and walked through in a recorded live session, with the recommendation and the roadmap

Each stage closes with the completed work delivered and documented in an end-of-stage report, with a live demo when you want one.

4. WARRANTY

The report reflects the state of the system at the time of the audit and the access we were given. If access to part of the system is not granted, that gap is stated explicitly in the report rather than assumed.

5. BILLING

No advance payment. Billing is agreed with the client: either by milestone or at the close of each sprint. The total price does not change, only how it is distributed.

Payment within 15 days of invoice · Intellectual property transferred on payment of the final invoice.

6. WHAT'S NOT INCLUDED

Any change to the system: the audit does not fix, patch or refactor anything · Penetration testing and formal security certification · Formal load testing · Audit of third-party systems the product connects to · Provisioning of access or credentials · Legal advice on licensing disputes · Video editing of the session recording · Data recovery

7. WHAT WE NEED FROM YOU

Read access to the repositories and to the running environments · One technical contact for questions · Up to three short interviews with the people who build or operate the system · Any documentation that exists, as it is. Missing documentation is a finding, not a blocker. Included revisions: 1 round of corrections on the draft report before it is issued as final.