

Sample document. Nordvantage Logistics SA does not exist. Every name, figure, command output and date is invented, to show what a delivered flochai audit summary looks like. The fact patterns come from real engagements with figures shifted and names removed.

Nordvantage Logistics SA

One-week platform audit, in summary. The full report runs to eleven sections, and every claim made here is evidenced there.

Review week 11-15 May 2026 · Report issued 20 May 2026 · Report version 1.0 · Check list 2026.1
Florian Chaillou · hello@flochai.com

1 HIGH FINDING NOTIFIED SAME DAY	3 + 5 MEDIUM AND LOW LISTED IN FULL	€7,164 PER YEAR ATTACHED TO NOTHING	3h 40m MEASURED RECOVERY PREVIOUSLY UNKNOWN	12/14 PLAN ITEMS YOUR TEAM CAN DO ALONE
---	--	--	--	--

01 The three that matter

- Your GitLab answers on a public address** while running 16.9.1, against which three advisories describing authenticated remote code execution are published and unpatched. It holds six variables the production deploy job uses. Reading them is enough to deploy to production from outside your network. **Half a day to close**, and it does not depend on the upgrade. R-001 · High · notified by phone 12/05
- A backup restore works, and takes 3 hours 40 minutes.** It worked, which is not a given. But the duration is a number nobody had, and your three runbooks carry three different assumptions about it. R-009 · Medium · measured on a disposable instance 13/05
- €597 a month buys nothing.** Eleven disks attached to nothing, six unattached addresses, snapshots and images under no lifecycle policy, and health-check lines at 38% of log ingestion. **Two hours to delete.** §7 · from the billing export

02 The register

ID	FINDING	LEVEL	EFFORT	WHO
R-001	GitLab public and unpatched, holding deploy credentials	HIGH	half-day + window	your team
R-002	Batched migration failing since 14/04, blocks the upgrade path	MEDIUM	days	your team
R-003	bastion-ops: 34 pending security updates, kernel included	MEDIUM	hours	your team
R-009	Measured recovery 3h 40m; runbooks assume faster and disagree	MEDIUM	hours	your team
R-004	Floating image tags: a rollback cannot name a known-good	LOW	half-day	your team
R-005	Pod requests one copy-pasted block; on Autopilot that is the invoice	LOW	days	flochai
R-006	Logs have no shared destination; triage starts by finding them	LOW	days	flochai
R-007	No environment exercises integrations off production	LOW	days	your team
R-008	No agreed recovery point; three runbooks assume three things	LOW	hours	your team

Levels are derived, not chosen. Each entry states a consequence class and a trigger-evidence grade, and the level is a lookup of the two. To move an entry up I have to produce evidence that moves it a cell. I cannot type a level.

Two conditions were rejected. Both were on my list on Tuesday and both were killed by their own counter-argument. They are printed in the full report with the argument that killed them, because a register that only ever grows is a sales document.

03 What this costs you, and what it need not

Cost is not risk, so none of this is in the register. Every figure comes from the billing export, compared month over month across the three months to 30 April, with usage growth separated out. The platform cost **€14,200 a month** on average across that window.

Removable now, with no argument against it. Each is a resource attached to nothing, serving no request.

WHAT	PER MONTH	PER YEAR
11 persistent disks attached to nothing, 2.4 TB	€310	€3,720
6 reserved static addresses, none attached	€33	€396
1.8 TB of snapshots under no lifecycle policy	€47	€564
890 GB of container images under no cleanup policy	€89	€1,068
Health-check lines, 38% of ingested log volume	€118	€1,416
Total	€597	€7,164

That is **4.2% of the monthly bill** and about two hours of work. It needs a decision from nobody.

Worth doing, but each needs a decision. The argument against each is stated in the full report rather than left for you to find.

WHAT	PER MONTH	PER YEAR
Staging serves no traffic for 128 of 168 hours a week	€740	€8,880
Cloud SQL one tier above what 90 days of CPU supports	€310	€3,720
No commitment against a steady-state floor of 62%	€980	€11,760
Total	€2,030	€24,360

Identified is not realised. €31,524 a year appears above. None of it is saved until someone does the work, and the second table costs engineering time to capture. Treat the first table as money and the second as a shortlist of decisions.

Two items are deliberately not costed: the Autopilot request sizing, where the direction is not uniform because two services need more, and the Kafka provisioning, where the floor set by partitions and retention has not been established. Quoting a saving before those are answered would be quoting a number I cannot defend.

04 What happens next

#	FIRST FOURTEEN DAYS	EFFORT	WHO
1	Delete the unattached resources, add lifecycle and cleanup policies, drop health-check lines from ingestion	2 hours	your team
2	Put GitLab behind IAP or the VPN	half-day + window	your team
3	Patch bastion-ops, enable security-pocket unattended upgrades	hours	your team
4	Run the leaver difference against the directory	20 min	your team
5	Write the recovery point objective against the measured 3h 40m	hours	your team + COO

The remaining nine items run to day 90 and are in the full report. **Twelve of the fourteen route to your team, not to me.** The two that do not name the capability rather than the company, so you can price hiring it against buying it.

05 How I am paid, and what I did about it

This audit is a fixed fee and it credits against the first month if it becomes a retainer. That gives this document a standing incentive to make your platform look worse than it is, and you should read it knowing that.

What you can check yourself: every level is a lookup of two stated inputs, so a level cannot be typed. The register came out one High, three Medium, five Low. Two conditions were rejected and are printed with the argument that killed them. One finding was demoted during Thursday's call and says so in its own entry. Twelve of fourteen plan items route to your team.

Corrections are free for 30 days from 20 May 2026. Every register entry carries a command you can re-run alone, so an entry that returns the same answer in six months, with nothing having fired, means I was wrong about it, and you do not need me to see that.