client document 02 · the savings audit

Security and data handling

The free first pass needs no access at all. The paid audit uses read-only access that you create, you can see, and you can remove at any time.

Step 1 (free): no access

You email a cost file (see *How to send your Azure cost data*). Nothing connects to your tenant.

Step 2 (paid audit): read-only access you control

How it's granted	You run one script, `grant-access.sh`, in Azure Cloud Shell. Read it first: it's under 100 lines. Public source: github.com/happycoding344/azure-audit-scripts at the fixed commit `d4c87aa8e689c23ffadd2cff37ec75240c4021cf`.
What it creates	One app registration, "cost-audit-naveenchandra", with roles on the subscriptions you name (every enabled subscription if you don't name any).
Roles	**Reader** (see resources, their settings, metrics and Advisor) and **Cost Management Reader** (see billing). Both are built-in Azure roles.
What it can't do	Create, change or delete anything. It can't read secrets, keys or connection strings (Reader can't run list-keys actions). It can't read the data inside your databases, storage accounts or VMs.
How long	The credential expires after **30 days**.
How to remove it	Run `revoke-access.sh` (same repository) or delete the app registration in Entra ID. Azure applies either within minutes, and a token issued just before expires within 90 minutes. We do this together at close.
How the credential reaches me	The script prints it once. Send it through a one-time secret link (for example onetimesecret.com), never in plain email.

What I collect, and where it goes

- **What I collect:** resource inventory and configuration, 14 days of platform metrics (CPU and similar), Advisor recommendations, and 90 days of cost data. I collect no application data.
- **Where it's kept:** only on my own encrypted laptop and an encrypted backup. No third-party tools process client data.
- **Who sees it:** only me. I don't share or sell it.
- **Retention:** deleted within **30 days** of the final report, or sooner on request. You get a written deletion confirmation.

Fixes

I don't make changes in your tenant. In the 2-hour fix session, **your engineer applies the changes** while I guide, using your normal change process. Any wider write access is agreed in writing, scoped to named resources, and time-boxed.

Paperwork before access

A mutual NDA and a services agreement are signed before the script is run.

If something goes wrong

If I suspect the credential or your data has been exposed, I'll tell you **within 24 hours**, and you revoke access straight away.

Contact: Naveen Chandra, contact@naveenchandra.co.in

Microsoft, Azure and Entra are trademarks of the Microsoft group of companies. Naveen Chandra is independent and not affiliated with Microsoft.