pravidha

Pramana

Product Overview

Governance evidence for Snowflake — classification, policy coverage, drift, audit packs

Document	Pramana — Product Overview
Version	v1.0
Date	17 November 2026
Author	Pravidha — Snowflake Select Service Partner
Status	Released
Classification	Public

© 2026 Pravidha. This document and the software it describes are Pravidha intellectual property.

Contents

In one paragraph
The questions it answers
How it works
Who gets what
What it takes
What it deliberately does not do
Trial and full version
Works with Vigil
Where to go next

© 2026 Pravidha · Public

For the people who decide whether Pramana is worth having: heads of data, data protection officers, risk and compliance leads, and whoever sponsors the platform. No Snowflake knowledge needed. About eight minutes.

In one paragraph

Pramana is an application that runs inside your Snowflake account and answers one question every night: is our sensitive data classified, protected, and reachable only by the people who should reach it? It answers with evidence. Each run produces a dated pack that says, control by control, what holds and what does not, mapped to the clauses of the frameworks you report against. It never reads the data in your tables and it never changes anything. What it finds, your own people decide what to do about.

The questions it answers

Most organisations can say what their data protection policy is. Far fewer can show, on a given day, that the platform matches it. Pramana closes that gap for Snowflake by answering the questions that auditors, regulators and your own board keep coming back to:

The question	What Pramana shows
Do we know where our personal and sensitive data is?	Every column that looks like personal, financial or health data, and whether it has been labelled as such
Is it protected?	Whether each labelled column is masked by the policy you chose for that kind of data, and whether tables that need row-level restrictions have them
Who can get to it?	Broad roles that can read sensitive tables, and sensitive tables owned by roles you do not consider accountable
Do we keep it only as long as we should?	Whether every table holding sensitive data carries a retention class, and whether that class is one you defined
Did anything get worse since yesterday?	What changed between two nights, with the changes that weaken your position listed first
Can we prove all of this, on a date of our choosing?	A sealed evidence pack per framework, kept for as long as you set

© 2026 Pravidha · Public

How it works



Figure 1 · *How Pramana works: read, compare, find, decide, evidence, every night*

Pramana reads Snowflake's own record of your account: which tables and columns exist, how they are tagged, which policies are attached, who has been granted what. It compares that with your **policy pack**, a small set of tables in which you state your intent: what counts as sensitive, which policy protects each kind of data, which roles are too broad, which retention classes exist.

The comparison produces a result for each of thirteen controls. Where a column looks sensitive and has no label, Pramana proposes one and a data steward approves or rejects it. Where something has to change, Pramana writes the exact statement and hands it to your change process. It does not run it.

At the end of each run it writes an evidence pack for each framework you have chosen. UK GDPR, DORA and ISO 27001 are mapped out of the box, and you can add your own.

Who gets what

If you are	Pramana gives you
A sponsor or head of data	One overall status, the number of failing controls and how much of each database is covered, in terms a board can read without translation
A data protection officer or compliance lead	Evidence by clause, the list of accepted exceptions with who approved each and until when, and a pack for any past date
A data steward	A queue of proposed classifications to approve or reject, and the changes that need a second look
A platform or governance engineer	Findings with the statement that closes each one, ready for your pipeline
An auditor	A read-only console, and packs you can take away and verify have not been altered

What it takes

- **A Snowflake account on Enterprise Edition or higher.** The features Pramana checks (tags, masking, row access policies, classification) are Enterprise features.
- **A few minutes of an account administrator's time, once.** Three grants let Pramana read the account's metadata. Nothing else is asked for.

© 2026 Pravidha · Public

- **No infrastructure.** Pramana brings no servers, creates no warehouse and needs no integration. It runs one scheduled job on Snowflake's serverless compute; a night's run is a handful of metadata queries.
- **A minute to see it working.** A sample estate with planted defects ships inside the application. It loads without any grant and shows every screen with something in it.

Setting it up on your own account is covered in Install and Setup.

What it deliberately does not do

Being clear about the edges is part of what makes the evidence usable.

- **It does not read your data.** It works from metadata. It can tell you that a column called `DATE_OF_BIRTH` is not masked; it has never seen a date of birth.
- **It does not change anything.** Every fix is a statement your own people run. An application that could alter your policies would itself be a risk worth auditing.
- **It is not a legal opinion.** A pack is evidence about technical controls on one platform. It supports a compliance position; it does not replace the judgement of the people accountable for it.
- **It is not instantaneous.** Snowflake's account metadata runs a few hours behind. Pramana is built for evidence produced nightly, not for live monitoring.
- **It checks that protection is in place, not what the protection does.** It proves the right masking policy is attached to a column. Whether that policy shows the right thing to the right person is yours to review.

Security and Trust sets out exactly what Pramana can reach and what it stores. The Evidence Guide explains how to read a pack and how far it can be relied on.

Trial and full version

The listing on the Snowflake Marketplace is a trial of the whole product. Nothing is switched off, and the trial runs for the period shown on the listing. When it ends, Snowflake suspends the application.

To carry on, select **Request** on the listing. Pravidha replies with terms and shares the full version with your account. Snowflake installs the full version as an application of its own, so it is worth knowing two things before a trial ends: your policy pack moves across as a set of files, and the evidence packs you want to keep should be downloaded first. Both take minutes, and Operations and Troubleshooting walks through them.

The full version is priced on request. Select **Request** on the listing, or write to **support@pravidha.com**.

Works with Vigil

If you also run Vigil, Pravidha's data quality and reconciliation application, Pramana can carry Vigil's reconciliation results in every evidence pack and flag a sensitive table that does not reconcile. Pramana stands on its own without it.

Where to go next

You want to	Read
Understand what Pramana can access, and what leaves your account	Security and Trust

© 2026 Pravidha · Public

You want to	Read
Read an evidence pack, or answer an audit request	Evidence Guide
Install it and run it for the first time	Install and Setup
Look up a word	Glossary

Questions: **info@pravidha.com**. Pravidha is a Snowflake Select Services Partner.