



MODULE 15

Audit Report Builder

A five-step wizard producing the database audit report, the QA/QC report or the integrated investor-grade report — with findings, recommendations and an action plan.

- Group: Integration
- HMAC-SHA256 signed audit log
- Restricted to administrators
- 3 report types · 10 sections

Executive summary

The Audit Report Builder answers a precise question: who changed what, when, and is the database sound? Five steps produce the database audit report, the QA/QC report or the integrated document intended for investors.

01 What it replaces

The audit note written by hand from screenshots, and the impossibility of proving a value was not modified after the fact.

02 How it works

You pick the theme, point at the sources — change history, connection log, per-user activity, integrity check — configure, preview and generate.

03 Who it is for

The quality manager, the competent person who signs, and the external auditor who asks for evidence rather than assertion.

3

report themes

5

wizard steps

105

tables covered by the integrity check

PDF + XLSX

signed deliverables

Contents

01 A restricted module

Reserved for top-level administration, invisible to standard roles.

02 Three report types

Database audit, QA/QC report, integrated investor report.

03 The five-step wizard

Type, sources, configuration, preview, generation.

04 Ten standard sections

From the executive summary to the action plan and conclusion.

05 Narrative tone

Balanced technical, audit committee, investor facing, operations and QA/QC.

06 Protected audit log

A separate SQLite database, HMAC signature verified on every open.

07 Compliance

Designed around the NI 43-101, JORC and PERC codes.

08 Business value

The audit file is produced, not reconstructed.



GeoMate 2026

SECTION I

The module

The problem addressed, the capabilities delivered, the processing chain and the module's place in the platform.

-
- 01 Context
 - 02 Key capabilities
 - 03 Processing chain
 - 04 Place in the platform
-

Context

A due diligence, an internal review or a security investigation ask the same question: who changed what, when, and has the database stayed consistent with its log.

The module answers by producing a dated, signed document, structured the way an audit committee expects — without any data leaving the workstation.

The log is tamper-evident

The <project>_audit.db file carries an HMAC-SHA256 signature verified on every open; an external modification raises an alert.

The tone adapts to the reader

Balanced technical, audit committee, investor facing or operations and QA/QC: the same substance, different writing.

The action plan is produced

Findings, recommendations and deadlines are generated from the anomalies actually detected, not from an empty template.

The screenshot shows the 'Audit & QA/QC Report Builder' interface at 'Step 3 of 5'. The left sidebar contains a navigation menu with five items: '01. Report Type', '02. Data Sources', '03. Configuration' (highlighted), '04. Preview', and '05. Generate'. The main content area is divided into three sections: 'REPORT IDENTITY', 'COMPANY LOGO', and 'PROFESSIONAL REPORT STYLE'. The 'REPORT IDENTITY' section includes fields for 'Author Name' (USER-01 — Database Manager), 'Project Name' (KOUKOUUDAN — Koukoudan N / Koukoudan C), 'Client / Company' (CLIENT A — Senegal), 'Report Date' (September 05, 2026), 'Report Number' (GM-AUD-2026-014), and 'Revision' (Rev. 1 — Issued for Review). The 'COMPANY LOGO' section has a 'Browse Logo...' button. The 'PROFESSIONAL REPORT STYLE' section includes 'Report Theme' (Executive Test) and 'Narrative Tone' (Investor facing). Below these is the 'REPORT SECTIONS' list, which includes 'Executive Summary', 'Objectives Scope', 'Methodology', 'Data Quality Assessment', 'QA/QC Analysis', 'Key Findings', 'Risk Assessment', 'Recommendations', 'Action Plan', and 'Conclusion'. At the bottom, there is an 'OPTIONS' section. Navigation buttons 'Back' and 'Next' are located at the bottom of the interface.

For projects subject to the NI 43-101, JORC or PERC codes, retaining the audit log for the full life of the project plus a minimum of ten years is recommended. Consult your Qualified Person for jurisdiction-specific requirements.

Key capabilities



01

Change history

Every insert, update and delete recorded with user, timestamp, table, field, old value and new value.



02

Login audit

Every authentication attempt — successful, failed, logout — with user id, role, timestamp and machine name.



03

Per-user activity

Per-account summary: pages opened, records modified, session duration, over any date range.



04

Integrity check

Comparison of the audit log against the current database state, to detect an unrecorded modification.



05

Three report themes

Professional formatting presets, with company logo, report number, revision and confidentiality marking.



06

PDF and Excel export

Timestamped signed PDF carrying the issuing account identifier, or an Excel workbook with one sheet per audit category.

Processing chain

From the raw trace to a signed audit file.

A Inputs

Traces and logs

- Change history of the database
- Connection log: who, when, from where
- Per-user activity and permissions in force
- Results of the integrity check across the tables
- Recorded QA/QC runs and their verdicts



B Assembly

Five-step wizard

- Theme choice: database audit, QA/QC or integrated
- Selection of the sources to include
- Configuration: period, scope, level of detail
- Preview of the whole document
- Generation with findings, recommendations and an action plan



C Outputs

A file that stands up

- Signed PDF report, theme as chosen
- Excel workbook of the detailed findings
- A dated, attributable action plan
- An exhibit for an external technical review
- A comparison baseline for the next audit

WHAT AN AUDIT ACTUALLY ASKS FOR

Not that the database be perfect, but that it be known what it holds, who changed it and under which checks. A documented finding beats an invisible problem: that is the report's logic, and why it includes recommendations and an action plan.

Place in the platform

FED BY

06 QAQC Manager

Supplies the recorded runs, their verdicts and their criteria.

05 Data Validation

Supplies the geological findings and the parameters applied.

Platform log

Change history, connections, activity and permissions.



Audit Report Builder

The evidence layer: it produces no data, it attests to how the other modules' data was obtained.

FEEDS

External technical review

The signed file is what the auditor or the competent person examines.

Investor file

The integrated theme produces the document for the investment committee.

14 Report Builder

The periodic report can cite the audit and its action plan.



GeoMate 2026

SECTION II

In practice

The real interface, the operating workflow, the reference settings, good practice and the questions that come up.

-
- 01 The interface
 - 02 Operating workflow
 - 03 In depth
 - 04 Good practice
 - 05 Frequently asked
-

The interface

Audit & QAQC Report Builder Step 3 of 5

01 Report Type
02 Data Sources
03 Configuration
04 Preview
05 Generate

REPORT IDENTITY

Author Name: USER-01 — Database Manager

Project Name: KOUKLOUDAN — Koukoudan N / Koukoudan C

Client / Company: CLIENT A — Senegal

Report Date: September 05, 2026

Report Number: GM-AUD-2026-014

Revision: Rev. 1 — Issued for Review

COMPANY LOGO

Browse Logo...

PROFESSIONAL REPORT STYLE

Report Theme: Executive Teal

Narrative Tone: Investor Facing

REPORT SECTIONS

- ☒ Executive Summary
- ☒ Objectives Scope
- ☒ Methodology
- ☒ Data Quality Assessment
- ☒ QAQC Analysis
- ☒ Key Findings
- ☒ Risk Assessment
- ☒ Recommendations
- ☒ Action Plan
- ☒ Conclusion

OPTIONS

Back Next

Actual GeoMate 2026 v2026.3.1.5 screen capture — Midnight theme.

1 Five-step wizard

Report type, data sources, configuration, preview, generation.

2 Report identity

Author, project, client, date, report number and revision.

3 Company logo

Embedded in the cover and the headers of the generated document.

4 Theme and tone

Executive Teal, and a narrative tone chosen for the intended reader.

5 Ten sections

Each section is independently selectable, from executive summary to conclusion.

Operating workflow

Five steps, and a signed document at the end.

1

Choose the type

Database audit, QA/QC report or investor-grade integrated report.

2

Point at the sources

Project database, supporting files and images to embed in the document.

3

Configure

Report identity, logo, theme, narrative tone and sections to include.

4

Preview

The report is rendered in the right panel before any file is generated.

5

Generate

Timestamped signed PDF, or an Excel workbook with one sheet per audit category.

Audit report types

TYPE	CONTENTS	READER
Database Audit	Complete audit of the drillhole database's integrity, consistency and compliance	Internal audit committee
QAQC Report	In-depth analysis of standards performance, blank contamination and field/lab duplicate precision	Qualified Person
Full Integrated Report	Combined audit and QA/QC executive report, with automated recommendations and an action plan	Investors and board

Sections and audit categories

REPORT SECTION	AUDIT CATEGORY COVERED
Executive Summary	Summary of findings and overall verdict
Objectives & Scope	Date range, tables, users and event types retained
Methodology	Rules applied, thresholds, data sources
Data Quality Assessment	Full change log: insert, update, delete with before and after values
QAQC Analysis	Standards, blanks and duplicates performance, batch verdicts
Key Findings	Anomalies detected, ranked by severity
Risk Assessment	Locked accounts, permission changes, unvalidated imports
Recommendations	Corrective actions proposed from the findings
Action Plan	Actions, owners and deadlines generated automatically
Conclusion	Overall position and any reservations

Good practice

The conditions of an audit file that stands up to a third party.

✓ Audit before, not after

An audit produced at an investor's request discovers; a periodic audit corrects. The second costs far less.

✓ Cover the full period

A report on a chosen quarter attests to nothing. The period must match the scope announced.

✓ Include the unfavourable findings

An audit with no findings is not reassuring, it is suspect. The action plan is what gives a finding its value.

✓ Have all three roles sign

Prepared, reviewed, approved: separation of roles is the foundation of the document's standing.

✓ Keep the workbook with the PDF

The PDF is the document, the workbook is the detailed evidence. One without the other is incomplete.

✓ Date and archive outside the database

An audit report stored only in the database it audits has no independence.

Frequently asked

The auditor's questions, and the audited team's.

Q What does the integrity check cover?

The database's tables, their internal consistency and the links between them — the technical counterpart of Validation's geological rules.

Q What separates the three themes?

The database audit covers the data and its history; the QA/QC one covers analytical quality; the integrated one combines both for an external reader.

Q Does the report prove nothing was modified?

It shows what the history recorded. Its value therefore depends on the continuity of that log — which is what an auditor checks first.

Q Can it be produced for a single prospect?

Yes: the scope is configurable. But a restricted scope must be announced as such in the document.

Q Should it be regenerated after correction?

Yes, and keep both versions: that is the record that the action plan was carried out.

Q Is this NI 43-101 or JORC compliant?

The report is review material, not a code report. Compliance rests with the competent person who uses and signs it.



GeoMate 2026

SECTION III

The data

What the module produces on a real dataset, and the vocabulary needed to read those results.

01 Anonymised data

02 Key concepts

Anonymised data

The auditable scope of a project the size of KOUKOUDAN.

12

GEOLOGISTS TRACED

authors identified on the campaign's collars

3

DRILLING CONTRACTORS

A (383) · B (241) · C (181)

224 712

AUDITABLE WRITES

each with author, timestamp and before / after values

HMAC-SHA256

LOG SIGNATURE

verified on every open of the module

On this campaign three drilling contractors and twelve geologists worked on the same database between 2009 and 2026. The audit log is what makes it possible, years later, to attach every record to its author and its date.

Source: KOUKOUDAN project database (Senegal) — figures computed from the real data exported from GeoMate.

Key concepts

The vocabulary of data audit.

Audit trail

The unbroken sequence of traces allowing who did what, and when, to be reconstructed. Its continuity is its value.

Action plan

The list of corrections to make, with an owner and a due date. It is what separates an audit from a mere survey.

Competent person

The qualified professional who takes responsibility for a published result, in the sense of the reporting codes.

Finding

A documented gap between what is and what should be. It calls for a recommendation and an action, not a justification.

Separation of roles

Prepared, reviewed, approved by three distinct people. The principle that makes a signature meaningful.

Integrity check

The verification that the database structure and the links between its tables are consistent — the technical counterpart of geological validation.



GeoMate 2026

SECTION IV

Value & specifications

What the module changes for the project, and its technical integration profile.

01 Business value

02 Technical profile

Business value

The audit file exists before the audit

The log is written continuously: the day the question is asked, the answer is already there.

Continuous log

Tampering is visible

The HMAC-SHA256 signature is verified on every open; an external modification of the log raises an alert.

HMAC-SHA256

The same substance, three readers

Audit committee, Qualified Person or investor: the narrative tone changes, the findings do not.

4 narrative tones

The action plan comes out of the report

Findings, recommendations and deadlines are generated from the anomalies actually present.

Generated, not written

Aligned with the reporting codes

Structure and retention designed around NI 43-101, JORC and PERC — recommended retention is project life plus ten years.

NI 43-101 · JORC

Technical profile

Log storage

File

<project>_audit.db, separate SQLite database

Signature

<project>_audit.db.sig, HMAC-SHA256

Verification

On every open of the module

Retention

Unlimited by default, configurable archiving

Audited content

Data

INSERT · UPDATE · DELETE with before / after values

Access

Successful and failed logins, lockouts

Permissions

Role assignments and page access

Imports

File, row count, author, validation outcome

Outputs

PDF

Signed, timestamped, issuing account identifier

Excel

One sheet per audit category

Themes

Professional presets, embedded logo

Access

Owner and Zeus roles only



One platform, from field to report

The “Audit Report Builder” module is one of the 19 modules of GeoMate 2026 — a single, fully offline platform covering the whole chain: database design, data entry, validation, QA/QC, dispatch, analysis and reporting.