



FOR SECURITY & ASSURANCE MANAGERS AND LEADS

Strengthen your assurance team. Keep control of your data.

Our innovation with AIS is a different take on AI for risk and assurance audits and reports. The AI assists, the auditor decides.

AIS strengthens auditors instead of replacing them, can run on local models so New Zealand data stays home, and produces every assurance output from one project record. Your seniors spend their time on judgement, your juniors grow, and every engagement carries a defensible audit trail.



Senior time on judgement

Less reformatting and chasing, more expert review.



Defensible outputs

Every rating linked to evidence, from one source of truth.



Independent review gates

No audit closes without sign off at each key point.



New Zealand data stays home

Runs in your environment, can use local AI models.

WHERE TEAMS LOSE TIME

- Work scattered across spreadsheets, Word and email
- Different documents built for every engagement
- Senior hours lost to reformatting and rework
- Juniors learning frameworks with little guidance
- Findings hard to track once the report is issued

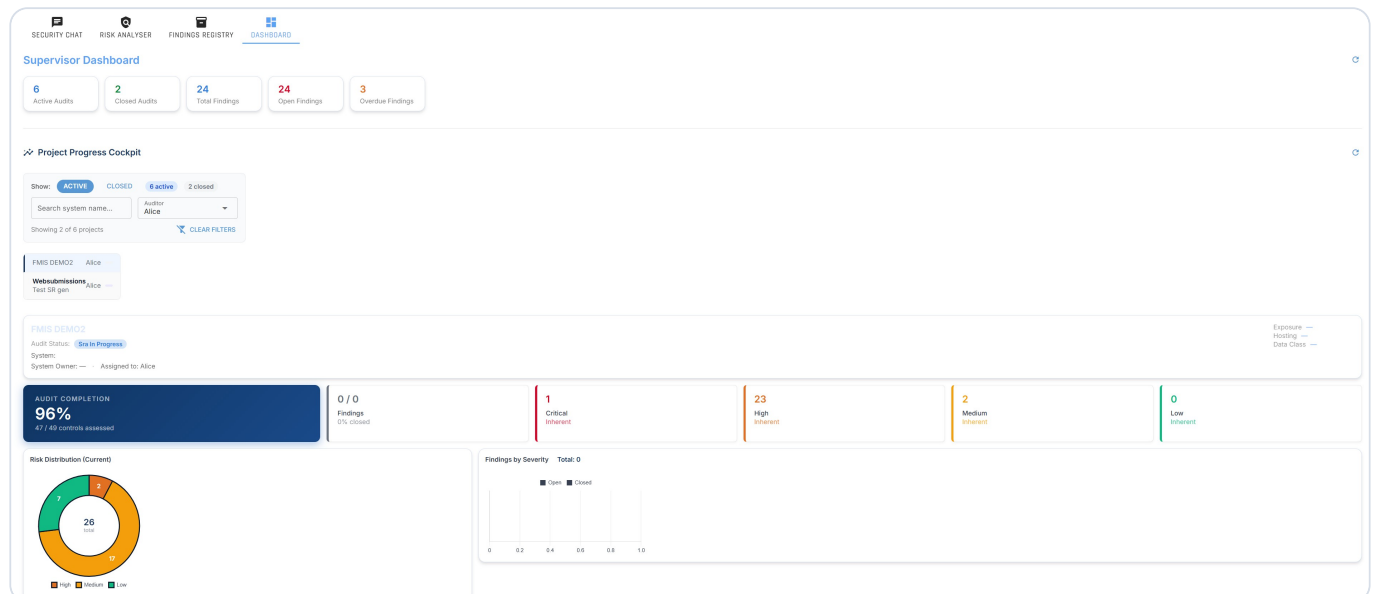


WHAT AIS GIVES YOUR TEAM

- One structured project record per engagement
- Every assurance output from the same data
- Checks that surface issues before review
- Guided assistance that builds junior capability
- A living registry that tracks findings to closure

Portfolio visibility for leads

assurance progress, findings by severity and risk position at a glance





What your team gets



More senior productivity

AIS catches inconsistent ratings, missing evidence and integrity issues before review. One record feeds all supported report types, so senior time goes to the assessment, not document preparation.



Higher quality outputs

Every control rating is linked to recorded evidence, and consistency checks run before review. AI helps draft risks, narratives and control guidance, but every draft is auditor reviewed before it enters the record. Scores reflect what auditors recorded, not AI inference.



Review gates before closure

Every audit passes through three formal gates: the Security Risk Assessment, the Control Validation Assessment, and a final review. At each one an independent reviewer is notified, checks the work and passes the gate. Nothing reaches closure without independent sign off.



Support that grows your juniors

Junior auditors get practical guidance in context: how to assess a control, what evidence to expect, whether evidence is sufficient and where gaps remain. They build skills on the job, while the final decision stays with the auditor.



Findings tracked after the audit

A Findings Registry covers every project. Each finding links to its control, risk and remediation plan, with owner, due date and status in the same record. Overdue items and patterns surface before they become accreditation problems.



Privacy and New Zealand data sovereignty

Sensitive security assessments should stay under the control of the organisation that owns them. AIS runs inside your environment, on premises or in your own cloud, and can use locally hosted AI models without relying on external AI services. Assessment data, framework databases and configuration stay within your environment, with no shared infrastructure between customers. Access is protected by role based controls, MFA and activity logging.

Runs on prem or your cloud

Local AI models

No shared infrastructure

RBAC + MFA

Full audit logging

Framework support

NZISM v3.9

NIST SP 800-53

ISO/IEC 27002

PSR Policy Framework

Privacy Act IPPs

Custom catalogues

See AIS on your kind of assessment

A walkthrough tailored to your sector, with realistic assessment data.

Book a demo

AIS supports NZISM and FISMA aligned assurance workflows. It assists auditors with drafting and review. It does not make accreditation decisions, accept risk, or guarantee compliance, certification or approval. Those decisions stay with authorised personnel.