Deis TECHNOLOGIES

CLIENT PROSPECTUS · 2026 · V2

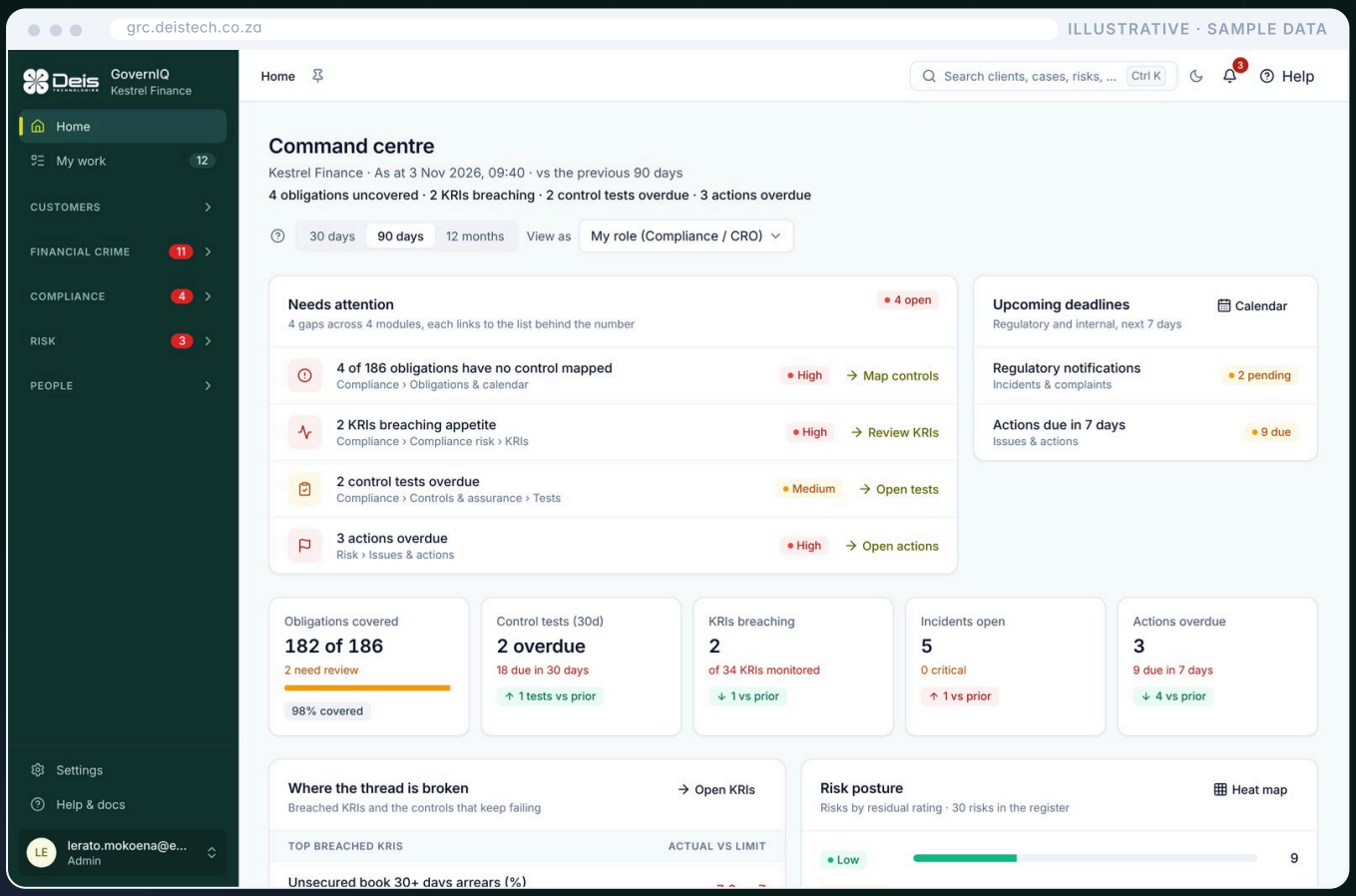
GOVERNANCE, RISK & COMPLIANCE PLATFORM

GovernIQ

Govern. Manage risk. Comply. One platform built around South African law, not adapted to it.

Risk management, compliance obligations, financial crime controls, onboarding, regulatory reporting and staff competence in a single connected system. Every risk links to its controls, every control to its tests and evidence, and every piece of evidence to the obligation it satisfies.

- Risk & assurance
- Compliance & RMCP
- KYC / KYB & UBO
- AML & goAML
- FAIS & conduct



PREPARED BY

Deis Technologies

ENQUIRIES

sales@deistech.co.za · +27 82 761 9921

WHY GOVERNIQ

Compliance fails in the gaps between the spreadsheets.

A risk lives in one workbook, the control that mitigates it in another, the test result in an inbox, and the evidence in a folder nobody can find at audit. The obligations register was last reviewed two cycles ago. The RMCP sits in Word. Nobody can say, on demand, whether a control that matters actually worked — and that is precisely the question a regulator asks.

GovernIQ replaces that with one connected record. Risks, controls, incidents, actions, obligations, policies, clients and cases live in the same system and reference each other. When a control fails a test, the risk it mitigates, the actions raised and the evidence trail are one click away.

28
Modules, switched on per organisation — start with what you need and add the rest without migration.

One record
Risks, controls, obligations, cases and evidence connected, not maintained in parallel.

Provable
Hash-chained audit trails, verifiable on demand, with four-eyes control on every sensitive decision.

GOVERNIQ REPLACES

Risk workbooks
Registers that drift apart between reviews.

Compliance calendars
Deadlines tracked by memory and email.

Point AML tools
Screening with no link to the case or the file.

Manual returns
Reports assembled by hand each cycle.

→ THE SHIFT

From compliance as a records exercise that is reconstructed before an audit, to compliance as a live state of the business — where “show me” is a query, not an archaeology project.

ONE PLATFORM

Seven domains. One connected system.

Each domain is useful on its own, and far more useful beside the others, because they share one organisation record, one obligation set, one evidence trail and one approval model.

Risk and assurance

Risk register, KRIs, risk appetite, heat maps, business risk assessments, controls, control testing, monitoring plans, audit engagements and evidence.

Compliance

Compliance wizard, obligations register, compliance calendar, policy library, RMCP under Directive 12, regulatory change and regulatory returns.

Financial crime

KYC and KYB onboarding, beneficial ownership, AML screening and cases, transaction monitoring, goAML reporting, FinSurv and Directive 8 screening.

Conduct and FAIS

Representative register, fit and proper, CPD, FSP licences, debarment, gift register, client suitability and product governance.

Operations

Incidents and breaches, complaints, issues and actions, licence to trade, insurance register, third-party and supplier risk, and workflow.

People

Training and awareness with a built-in course library, attestation campaigns, declarations and employee screening.

PLATFORM

A single work inbox that gathers everything waiting on a person from thirteen sources, notifications and reminders, document management, bulk imports and exports, saved register views, global search, a partner API with scoped keys and outbound webhooks, usage metering and administration.

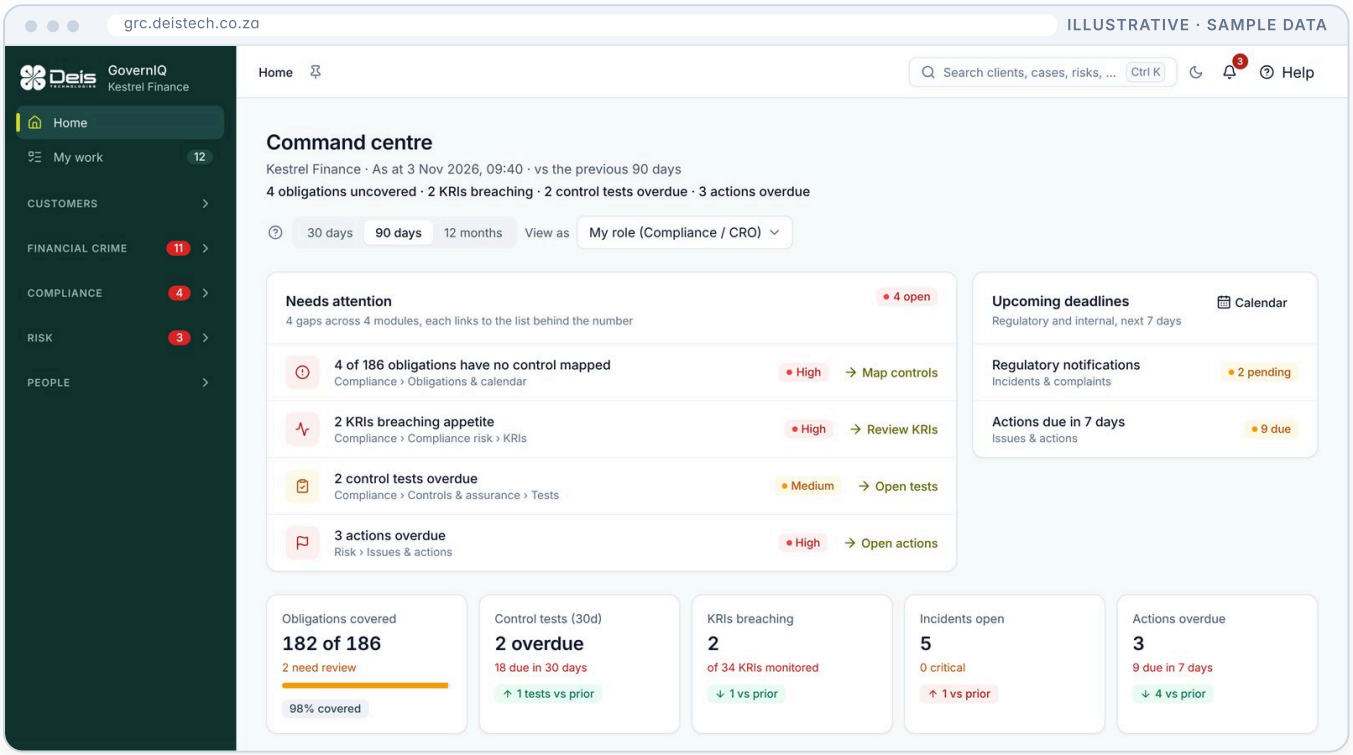
Switch on only the modules you need

A small financial services provider can start with the compliance wizard and FAIS. A larger institution can run the full financial crime suite. Modules are added at any time, without migration or re-implementation.

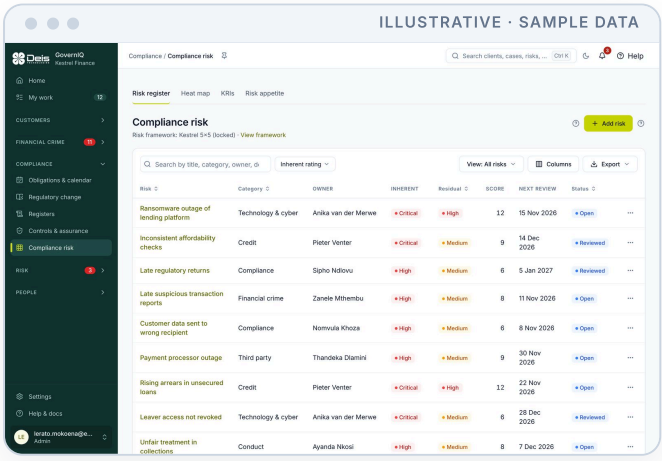
GOVERNIQ, AS YOUR COMPLIANCE TEAM USES IT

The gaps that need attention, linked to the list behind them.

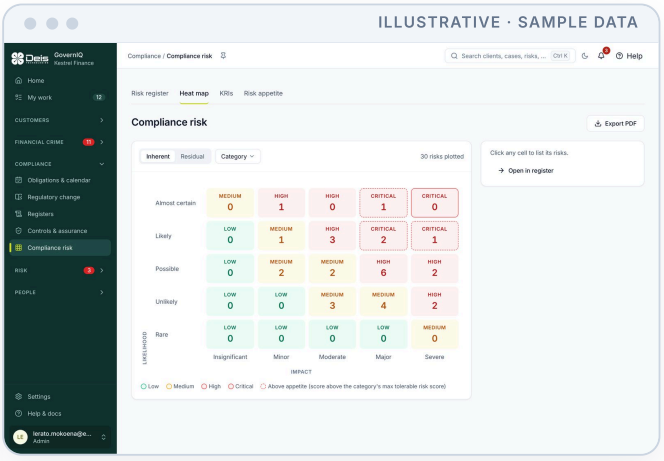
The command centre opens on what needs a decision: obligations without mapped controls, KRIs breaching appetite, overdue control tests and actions — each number one click from the records behind it.



Command centre. Obligations covered, control tests, KRIs breaching, incidents open and actions overdue, with upcoming deadlines alongside.



Risk register. Every risk with its owner, inherent and residual rating, score and next review.



Heat map. 30 risks by likelihood and impact, with appetite breaches outlined.

Screens are captured from the live product with a fictional client, Kestrel Finance. Every name, company and figure shown is sample data.

RISK, CONTROLS AND EVIDENCE

Prove the control worked, not just that it exists.

A complete cycle from risk identification to board reporting, with the control testing and evidence that turns an assertion into something an auditor can accept.

ENTERPRISE RISK MANAGEMENT

- **Risk register** with assessments, mitigations, full change history and cost-benefit analysis behind each treatment decision.
- **Your own risk framework** — define likelihood and impact scales, the matrix, categories and financial bases, so a score means the same thing everywhere.
- **Heat maps** that show the shape of the risk profile at a glance.
- **Risk appetite statements** that set the limits the business has agreed to work within.
- **Key risk indicators** with measurements recorded over time.
- **Business risk assessment** documenting the institution-wide ML/TF assessment the FIC Act requires.
- **Ownership-based permissions** — risk owners manage their own risks, risk managers manage any risk.

CONTROLS AND ASSURANCE

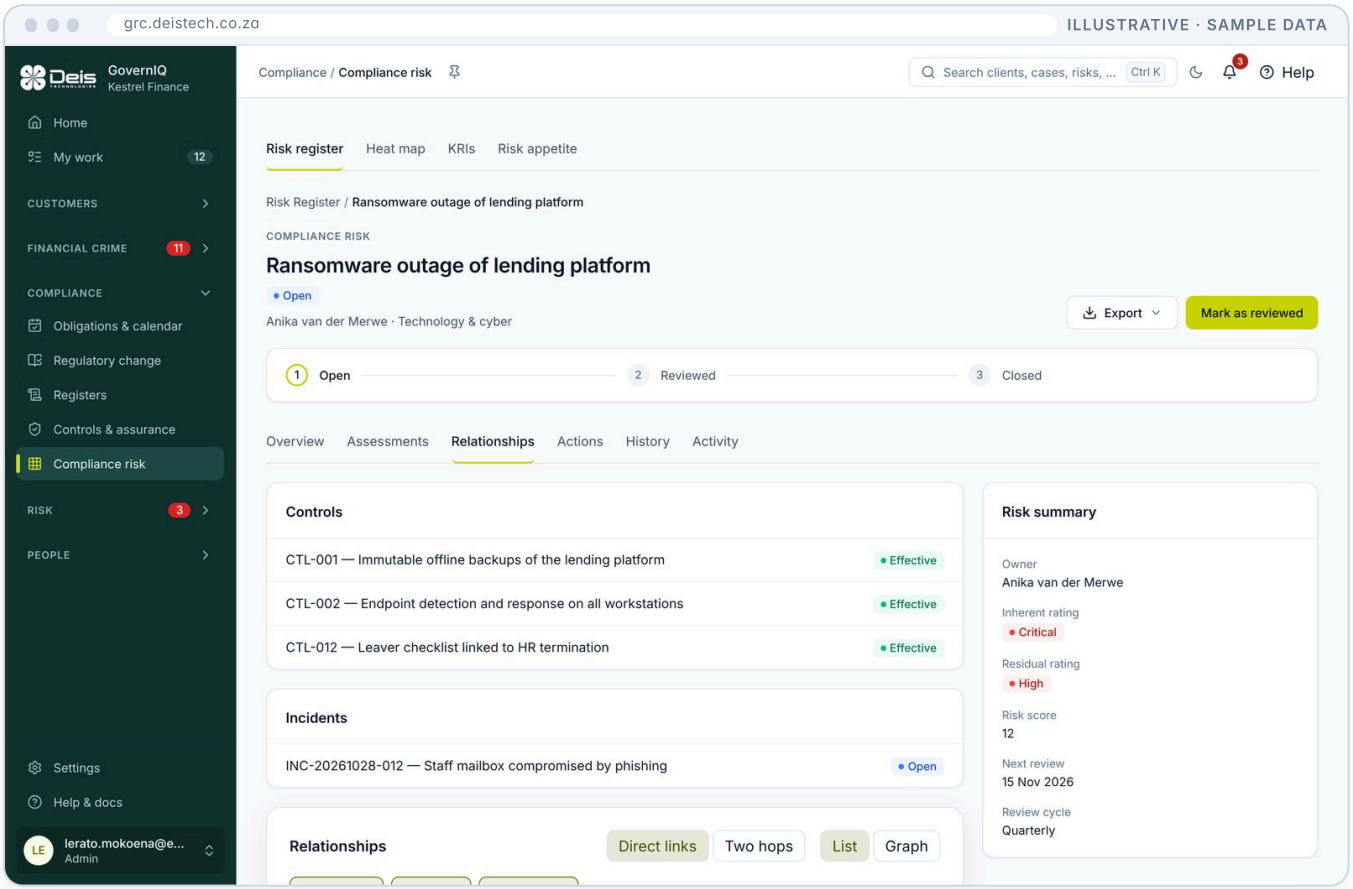
- **Control library** linked to the risks each control mitigates, with a coverage matrix that exposes risks with weak or missing controls.
- **Control testing** with recorded results, and evidence requests that chase control owners for proof through submission, acceptance or rejection.
- **Monitoring plans** that schedule ongoing monitoring, record findings and turn findings straight into actions.
- **Audit engagements and workpapers** with separate preparer and reviewer sign-off.
- **Versioned evidence** items and packs, ready to hand to an auditor or a regulator.
- **Access certification campaigns** where managers certify, revoke or delegate access, with revocations applied and recorded.

> A control register tells you what you intended. A tested control with accepted evidence tells you what actually happened — and only one of those survives an inspection.

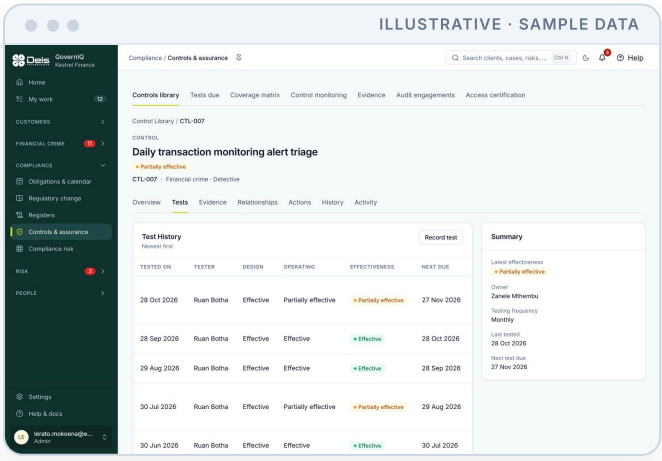
FROM THE REGISTER TO THE PROOF

A risk, its controls, their tests and the evidence — one record.

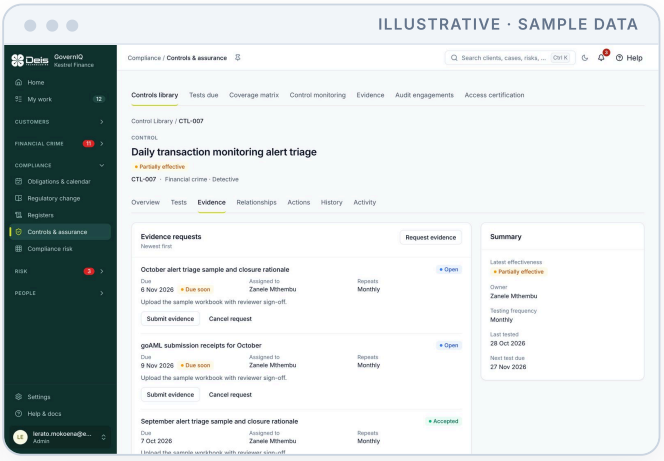
Open a risk and its linked controls and incidents are on the same screen. Open a control and its test history and evidence requests are there too, so the answer to “did it work?” is never more than a click away.



Risk detail. A risk with its linked controls and their effectiveness, the related incident, and the risk summary alongside.



Control testing. Test history with design and operating results, effectiveness and the next test due.



Evidence requests. Proof chased from the control owner, from request through submission to acceptance.

INCIDENTS, COMPLAINTS, ISSUES AND ACTIONS

Tracked to closure — by a second person.

What went wrong, who complained and what has to be done next sit in the same record as the risks and controls they touch, so every follow-up has an owner, a due date and an independent check at the end.

Incidents and breaches

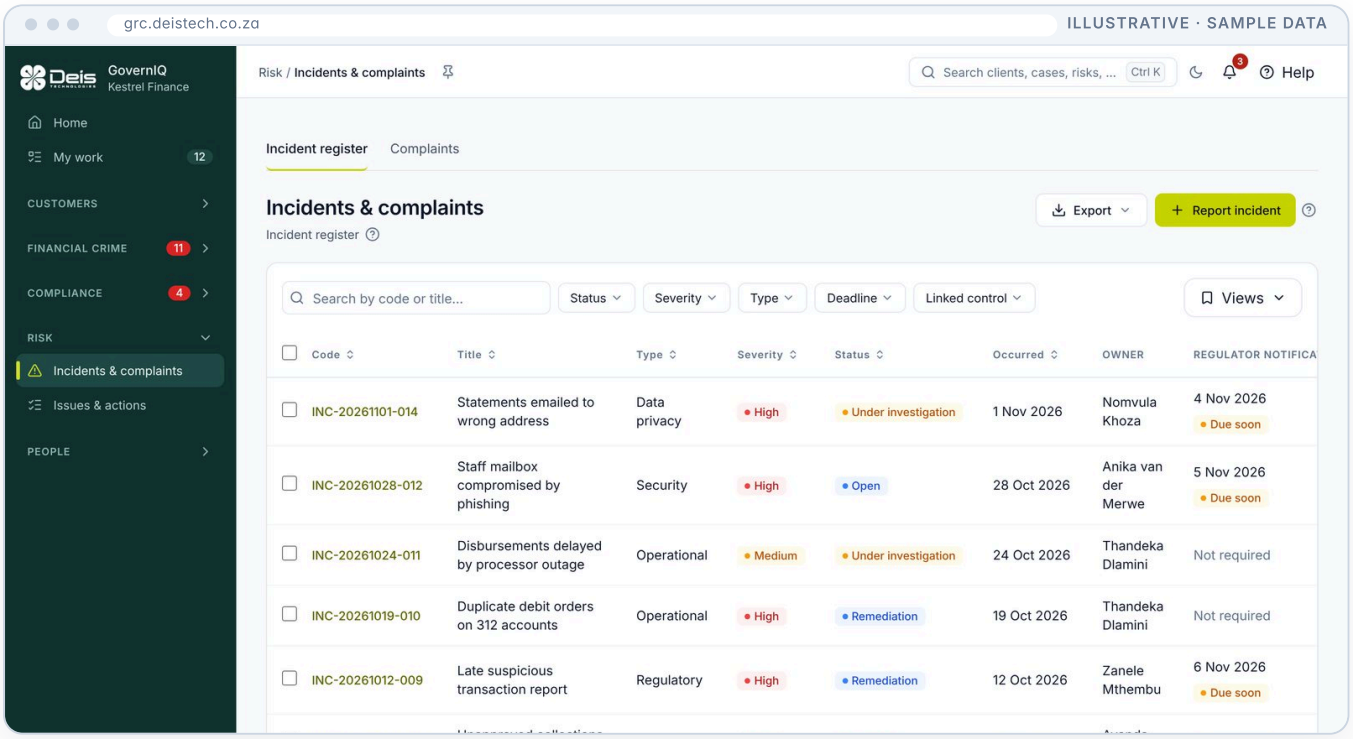
A structured lifecycle with linked corrective actions and a record of notifications made to regulators and affected data subjects. An incident cannot be closed while required steps remain open.

Complaints

Logged, tracked through status and summarised, so a pattern in complaints becomes visible rather than anecdotal.

Issues and actions

Owners, due dates, “my actions” and “overdue” views and bulk reassignment. Nobody verifies their own action, so closure always involves a second person.



Incident register. Type, severity, status, owner and regulator notification for every incident, filterable and exportable.

Connected, not logged in parallel

Incidents, complaints, issues and actions reference the risks, controls and obligations they touch. When a control fails a test, the risk it mitigates, the actions raised and the evidence trail are one click away.

FROM “WHICH LAWS APPLY TO US?” TO A WORKING PROGRAMME

Obligations you can defend, policies you actually keep.

A guided profile establishes what the business does, where and how. Deterministic rules — reviewable, explainable, never a language model — then decide which obligations apply, and the calendar, policies and attestations follow from there.

1. **Build the company profile**
   Five guided steps capture the entity, its activities, jurisdictions, clients and channels.
2. **Determine applicability**
   Transparent rules work out which obligations apply. Anything marked not applicable carries a recorded reason.
3. **Populate the register and calendar**
   Obligations get status tracking and deadlines, with reminder notifications ahead of each one.
4. **Generate the policies**
   Word documents produced from templates, branded with your officers, approval matrix, logo and letterhead.
5. **Attest and maintain**
   Staff read and confirm policies through attestation campaigns; regulatory change updates the obligations behind them.

POLICY LIBRARY

Catalogue with recommendations

Policies suggested from your organisation’s profile, with a preview before you commit to one.

Full lifecycle with approval

Submit, return, approve, reject, activate, revise and archive — with maker-checker approval on the step that matters.

Attestation campaigns

Ask staff to read and confirm, with each person’s attestations visible to them in one place and exportable for the record.

AI assists. Rules decide.

AI explains obligations in plain language, drafts policy prose and suggests RMCP content and controls — all of it reviewed and accepted by a person. Whether an obligation applies to your business is decided by deterministic rules that can be inspected and explained, never by a model.

FIC DIRECTIVE 12

An RMCP that is a programme, not a document.

The risk management and compliance programme is structured into the nine areas Directive 12 sets out, drafted section by section, approved, versioned, filed on schedule and attested by staff — with a coverage view that links the programme back to the obligations and controls it depends on.

THE NINE PROGRAMME AREAS

- 1 Scope
- 2 Risk-based approach
- 3 Customer due diligence
- 4 Ongoing monitoring
- 5 Reporting
- 6 Record keeping
- 7 Screening
- 8 Training
- 9 Governance

Drafting and approval

Section-by-section drafting with acceptance and approvals, generation of the final programme document, and a history of every version produced — so you can show what the programme said on any given date.

Filing schedule

A schedule driven by Directive 12's submission requirements, with filing records kept against each cycle.

Coverage view

Links the programme to the obligations it answers, the activities it governs and the effectiveness of the controls behind it — so a gap in the programme is visible before an inspector finds it.

Staff attestation

Attestation campaigns on the approved programme, tracked per person and exportable as evidence of training and awareness.

REGULATORY CHANGE AND RETURNS

Regulatory universe

Browse the full set of obligations the platform tracks, with the source and the test for applicability visible.

Change register

New and amended requirements are recorded and each change is linked to the obligations it affects, so impact is traceable rather than estimated.

Regulatory returns

A register of submissions with status and CSV export, so the reporting record is one list rather than a folder of attachments.



WHY IT MATTERS

Directive 12 does not ask whether you have an RMCP. It asks what is in it, when it was approved, who approved it, what has changed since, and whether your staff know it. GovernIQ holds the answer to each of those as a record, not a recollection.

CUSTOMER DUE DILIGENCE

Onboarding configured once, then governed.

A configurable onboarding engine for individuals and companies, built on the FIC Act's customer due diligence requirements. Every case carries a complete pack, an event history and a record of where each piece of information came from.

Case management

Review, assign, comment, re-run or override checks, expire and renew for re-KYC. The pack, the history and the provenance of every field travel with the case.

Requirements engine

A South African requirements catalogue with risk-based profiles, organisation-specific overlays and conditional logic. Configuration changes are published through maker-checker approval.

Visual onboarding designer

Build and adjust onboarding journeys visually, so a change to a journey is a configuration decision rather than a development request.

Applicant capture portal

Send applicants a secure link where they give consent, complete their details, upload documents and answer requests for information — without needing an account.

Company search and KYB

Search and verify against company registry data, with verification checks run through integrated providers and assembled into the case file.

Standalone checks and command centre

Run one-off checks outside a full case, and keep an overview of all onboarding work in progress in a single command centre.

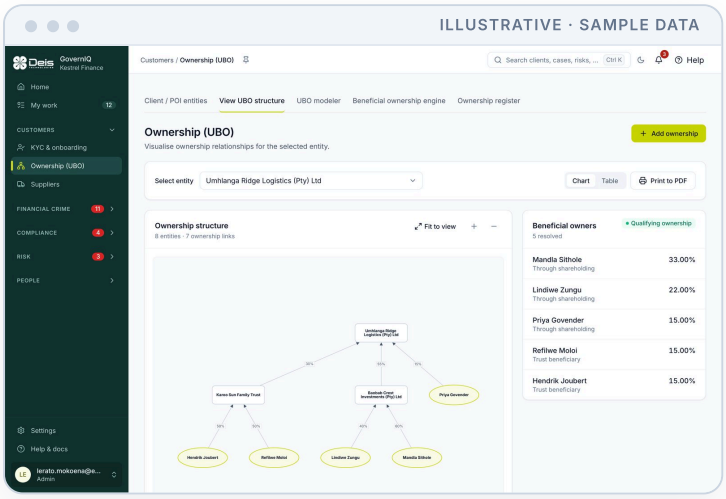
Requests for information, in the case

Missing details are collected from the applicant through a tracked RFI rather than an email thread, so the gap, the chase and the answer all sit inside the file the reviewer is working from.

UBO

Find the natural person — and show how you got there.

Identifying who ultimately owns or controls a legal entity is only half the obligation. The other half is documenting how you reached that conclusion, in a form that survives the question six months later.



Interactive ownership graph. The full structure drawn out, so a chain that is hard to describe in a memo becomes obvious on screen.

STRUCTURES THE ENGINE RESOLVES

- **Multi-layer holdings** — companies holding companies, to any depth.
- **Trusts** — founders, trustees and beneficiaries as roles.
- **Foreign entities** — offshore layers carried through the calculation.
- **Control without equity** — senior management and other means of control.

Ownership structures

Companies, trusts and other entities across multiple layers, including trust roles, senior management and control exercised through other means.

Determination engine

Compounded indirect ownership calculated through every layer, then control and senior-management tests applied in the order the guidance sets out. Each result carries a reason code and its supporting evidence.

Determination pack

A PDF that documents the outcome and the reasoning for auditors and regulators — the file you hand over rather than the explanation you improvise.

HOW A DETERMINATION RUNS

01 Capture the ownership structure and roles

02 Compound indirect holdings through each layer

03 Apply the ownership threshold test

04 Apply control and senior-management tests

05 Produce the pack with reasons and evidence

Tamper-evident by construction

The beneficial ownership audit log is hash-chained and verifiable on demand, so an altered record is detectable rather than merely unlikely. The same applies to AML case trails.

SCREENING, CASES AND MONITORING

Alerts become cases. Cases need two people.

Screening and monitoring are only as good as what happens after the alert. GovernIQ takes every alert through a governed workflow where the person who proposes an outcome is never the person who approves it.

AML SCREENING AND CASES

- **Sanctions and PEP screening** of clients and suppliers through an integrated screening provider.
- **Alert handling** — dismiss with a reason, or promote the alert into a case.
- **Case workflow** with assignment, comments, status transitions and the ability to exclude a false-positive hit with a recorded reason.
- **Four-eyes disposition** — one person proposes the outcome, a second approves or rejects it.
- **Tamper-evident case trail**, verifiable on demand.

TRANSACTION MONITORING

- **Flexible ingestion** — upload CSV or Excel, or submit through the partner API. Files can be validated without loading anything; rejected rows come back in an errors file and duplicate submissions are detected.
- **Tunable per organisation** with a full history of changes and a simulation that previews the effect before you save. Statutory limits cannot be relaxed beyond what the law allows.
- **Alert queue** with assignment, comments, four-eyes closure and escalation straight into an AML case.
- **Transaction capture** with maker-checker authorisation and recurring schedules.

TWELVE MONITORING RULES, OUT OF THE BOX

Large single transaction	FIC Act s28 cash threshold	Structuring	Velocity
Deviation from normal behaviour	High-risk jurisdictions	High-risk clients	Round amounts
Dormant account reactivation	Rapid movement of funds	Large transactions by new clients	Manual flags

THE THRESHOLD KNOWS THE NUMBER

The cash-threshold rule is built around the FIC Act section 28 limit of R49,999.99, not a figure someone typed into a spreadsheet and forgot to maintain. Statutory values live in the platform and move when the law does.

GOAML · FINSURV · DIRECTIVE 8

Reports in the regulator's own schema.

Reporting is where a compliance programme is finally examined. GovernIQ produces filings in the formats the FIC and the SARB actually accept, drawn from the monitored transactions and cases already in the system.

GOAML · FIC

Suspicious and cash reports

STRs and unusual transaction reports under section 29, cash threshold reports under section 28, and terrorist financing and property reports under POCDATARA. Transactions are selected for an STR directly from monitoring.

GOAML · XML

Schema-correct generation

goAML XML produced in the FIC's own schema and ready to upload to the FIC portal, with a record kept of every filing made and the reporting entity's registration held centrally.

SARB · ADLA

FinSurv reporting

For authorised dealers with limited authority: FinSurv uploads and downloads validated against the SARB schemas, transaction and account imports, reconciliation runs with exception reporting and export, and checksum downloads.

DIRECTIVE 8 — EMPLOYEE SCREENING

Directive 8 obliges every accountable institution in Schedule 1 of FICA to screen employees for competence and integrity, before appointment and then on a risk cycle. GovernIQ runs that as a managed, recurring programme rather than a once-off project.

Assessments and checks

Employee risk assessments with submit, approve, reject and rework steps, and required checks and interventions tracked per employee.

Sweeps and rescreening

Sanctions screening sweeps across staff, and rescreening of employees who are due or overdue — raising actions automatically where something needs attention.

Declarations and reporting

Employees complete declarations through a secure link; batches screen groups of staff at once, and the compliance report is produced as a PDF for the personnel file.

Screening intensity proportionate to the role

The case engine holds a screening profile per risk class and triggers each rescreen automatically, so the cycle the directive expects runs without anyone maintaining a reminder list.

FINANCIAL SERVICES CONDUCT

Representatives, suitability and the licence behind them.

Everything a financial services provider needs to manage its representatives, evidence fit and proper, keep CPD current and stay licensed — alongside the client suitability and product governance that conduct supervision now expects.

FAIS COMPLIANCE

- **Representative register** with qualifications, certifications, professional memberships, work experience, class of business and financial-services categories.
- **Fit and proper** — declarations, outcomes, a summary per representative and an at-a-glance indicator.
- **Continuing professional development** — activities with verification, points and certificates per CPD cycle, logged by representatives themselves through a self-service area.
- **Supervision**, regulatory exams, product training and compliance monitoring records.
- **Key individuals, FSP licences** and licence conditions, with the debarment process and register and a gift register alongside.

CLIENT SUITABILITY

- Versioned risk-profile questionnaires for attitude to risk and capacity for loss, which can be published, imported and exported.
- Suitability assessments that run from completion to an agreed risk profile and a final report.
- Client self-service links so clients complete questionnaires themselves.

PRODUCT GOVERNANCE

- Product register with status and an approval committee process.
- Risk assessments and periodic reviews linked to risks and KPIs.
- Mandate limits with recorded readings, including CSV upload, and breach tracking.

STRATEGIC RISK AND BOARD REPORTING

Strategic objectives

Linked to the risks and KPIs that affect them.

Roll-up

Operational risks aggregated into strategic risks.

Quarterly snapshots

Movement between quarters, finalised for the record.

Board pack

Board view with Excel export, plus scenario analysis.

OPPORTUNITIES, NOT ONLY RISKS

An opportunity register sits alongside the risk register — including opportunities raised directly from a risk — with expected benefits and history, so the same framework that records what could go wrong also records what is worth pursuing.

THE WORK, AND WHERE IT LANDS

One inbox for everything waiting on a person.

Compliance work fails quietly when it is spread across thirteen screens and nobody owns the queue. GovernIQ gathers it into one place, with a team view for managers and reminders that arrive before the deadline rather than after it.

Work inbox from thirteen sources

Access reviews, actions, AML cases and dispositions, attestations, control tests, evidence requests, incidents, KYC cases, monitoring findings, RFI responses, training and workpaper reviews — in one list, with a team view for workload.

Notifications and reminders

Read and dismiss, notification rules and email digests, plus reminders for the compliance calendar, policy reviews, licences, supplier contracts, FAIS CPD and supervision.

Third-party and supplier risk

Supplier register with categories and sanctions screening, contract register with export, a tiering questionnaire that sets each supplier's risk tier with a material-outsourcing flag and POPIA operator-clause checks, and renewal reminders.

Training and awareness

A library of 28 courses and 54 microlearning modules across AML/CFT, POPIA, cyber security and ethics, with versioning under compliance-controlled publishing, group assignments, certificates and enrolment export.

Partner API and webhooks

A partner API for companies, KYC and KYB sessions and transactions, with scoped read or write keys that are stored securely and rate-limited, and outbound webhooks with test pings and a delivery log.

Documents, imports and exports

Professional PDF, Word and Excel outputs, bulk imports with templates and error resolution, exports across every register, saved register views, global search and record comments with mentions.

Administration without a project

Invite users one at a time or in bulk, assign built-in or custom roles with fine-grained allow and deny permissions per module, and follow a guided onboarding checklist that flags setup gaps before they become support calls.

SECURE BY DESIGN

A compliance system has to be compliant itself.

GovernIQ holds the most sensitive records a regulated business keeps. It is built so that isolation, encryption and approval are properties of the system rather than instructions in a manual.

Azure SA
Deis cloud runs in the Microsoft Azure South Africa North region, with no public network access to the database.

Per-tenant
AES-256-GCM encryption with a separate, rotatable data key for every organisation.

14,000+
Automated backend and frontend tests, with every migration applied to a real SQL Server in CI.

CAPABILITY	HOW GOVERNIQ DELIVERS IT
Data isolation	Every organisation's data is separated at the database level. If the system cannot establish which organisation a request belongs to, it returns nothing rather than risk returning someone else's data.
Encryption	Identity documents, two-factor secrets and integration secrets are encrypted with AES-256-GCM using a separate data key per organisation, protected by a master key in Azure Key Vault and rotatable.
Sign-in	Two-factor authentication with an authenticator app and backup codes is enforced by default. Microsoft Entra ID single sign-on is supported, and every administrator reset is audited.
Access control	Module entitlement plus fine-grained permissions per module and sensitive operation, with deny rules that always win.
Four-eyes control	Maker-checker on AML dispositions, transaction authorisation, alert closure, Directive 8 assessments, policy approval, onboarding configuration, evidence, workpapers, product approvals and access certification.
Audit trail	Every security-relevant operation is logged with field-level change history and sensitive values redacted. UBO and AML case trails are hash-chained and verifiable on demand.
Traceability	Every request carries a correlation ID, returned with every response, so any issue can be traced end to end.
Data minimisation	Retention jobs prune provider call logs, change history, expired tokens and idempotency records, and redact AI usage logs.
Certification	ISO 27001 and SOC 2: in progress.

> “The question a regulator asks is never “did you have a control?” — it is “show me who approved it, when, and on what evidence”. GovernIQ is built so the answer is a query.

REGULATORY COVERAGE

Grounded in the law you are actually measured against.

Financial crime

Financial Intelligence Centre Act 38 of 2001 — customer due diligence (sections 21 to 21H), beneficial ownership, reporting (sections 28 and 29) and the RMCP (section 42). FIC Directive 12, Directive 8 and Guidance Note 7B. POCDATARA, POCA and PRECCA. The General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Act 2022. The goAML reporting schema and SARB FinSurv reporting for ADLAs.

Conduct, data and corporate

FAIS including fit and proper and CPD; the Financial Sector Regulation Act, CISCA, Pension Funds Act, National Credit Act, National Payment System Act and Banks Act. POPIA including operator agreements, and the PAIA manual. The Companies Act beneficial ownership register, tax and B-BBEE legislation, and the employment and health-and-safety Acts. Environmental, water, air quality, waste and mineral resources legislation for licence-to-trade tracking.

GETTING STARTED

Your first ninety days, in five guided steps.

1
Organisation profile
Tell GovernIQ who you are and how you are regulated.

2
Choose modules
Switch on only the domains you need.

3
Roles and users
Invite your team with the right permissions.

4
Obligations and policies
Load your obligations and generate policies.

5
Go live
Start testing controls and collecting evidence.

A live setup checklist covers modules, two-factor settings and the first administrator, and organisation health warnings flag any gap before it becomes a problem.

Where it runs

Run GovernIQ in our South African cloud, on Deis infrastructure, or in your own environment — on premises or in your cloud. When GovernIQ runs in your infrastructure, your registers, evidence and case files stay in your environment.

NEXT STEP

Let’s map this to your obligations.

Tell us what your business does and which licences it holds, and we will show you the obligations the platform would raise, the modules that answer them, and what a first ninety days looks like — with GovernIQ running on a sample register.

PRICING

Call for a quote.

GovernIQ is priced to your needs — the modules and users you switch on, your volumes and where it is deployed. We confirm a quote after a short scoping call.

sales@deistech.co.za
+27 82 761 9921

WHAT WE SCOPE WITH YOU

- Which domains you need: risk, compliance, financial crime, conduct, people.
- Number of users and business units.
- Which regulators and reports you work with.
- Where you want it deployed: Deis cloud, Deis infrastructure or yours.

CALL
+27 82 761 9921

SALES
sales@deistech.co.za

WEB
deistech.co.za

LINKEDIN
linkedin.com/company/112186007

© 2026 Deis Technologies · GovernIQ · Governance, risk & compliance