ElevateX

NAVIGATE COMPLEXITY. ACHIEVE ASSURANCE.

Company and services overview

One team for governance, risk, compliance, legal, cyber security and software development, from the law that binds your business to the systems that carry it.



100+	15+	4	25+
CLIENTS SERVED	INDUSTRIES	COUNTRIES	LAWS AND STANDARDS

Our approach

You will never climb alone.



Above the tree line, the path gives out. The markers you were following vanish under fresh snow, and the summit you were promised becomes a rumour. In the office it looks different and feels the same. A new regulation lands on your desk. An auditor asks for evidence nobody can find. And with them comes the quiet fear of being a long way from help.

Every climb has a moment when people turn back. The weather closes in, the budget runs thin, and the plan that looked so clean in spring meets the ice. That is usually when you learn who you are really climbing with.

We are ElevateX, and we are the people you find beside you at that moment. Think of us as your sherpas, a word we borrow with respect.

In 2019 the Nepali mountaineer Nirmal Purja, known as Nims, set out to climb all fourteen of the world's peaks above 8 000 metres in seven months, when the record stood at nearly eight years. He did it in six months and six days, and he made sure the world saw the Nepali climbers, many of them Sherpas, who made it possible. Their generations at altitude, and a gene variant the press calls the super-athlete gene, let them carry the loads and fix the ropes that get everyone else to the top.

That is the work we do for you. Our legal and compliance consultants, cyber security specialists and software developers work as one team to help you meet the laws and standards that bind you. We have walked these routes with more than 100 clients, in more than 15 industries and four countries.

Knowing the mountain is only half of it. The other half is who walks with you. We do not hand you a map and wave from base camp. We rope up with your own people, in your offices and on your calls, from the first uncertain step. We learn how your business works day to day, then find a practical way through, one that often leaves you with clearer reporting and sometimes a lower cost, in place of a binder of theory. Where it helps, we bring what we have already built, including our own compliance platform, JARVIS, so you do not start from nothing.

You will feel us beside you in the everyday: straight answers to your questions, and your deadline carried as though it were ours. And while you climb, one of us is always looking further up the slope for what is coming next, the new laws, standards and technologies that will shape the route ahead.

The mountain will still be there in the morning. You will simply not face it alone.

Let's summit together.

Our values

What you can count on.

Eight principles shape every engagement, and you can hold us to each of them.

1 A team at the forefront

We keep pace with new laws, new standards and new technology, AI among them. Our work across many industries and several countries means we bring you what has worked in practice, ready to put in place.

2 Practical, not theoretical

We take the time to understand your business, then find the practical, logical way to comply. The aim is more than a ticked box: clearer reporting and visibility, less effort and, often, lower cost.

3 Professional and hands on

You work with people who know both the law and the technology. They work beside your team rather than at arm's length, and they keep their word.

4 We have done it before

Much of what you need, we have built and used before: JARVIS, our compliance platform, and a defined method for every service. You start from something that already works, which saves you time.

5 One team, the whole route

Legal, compliance, security and software sit in one firm, so you do not manage the gaps between separate advisers.

6 Builders as well as advisers

What we advise on, we can also build: AI automations, software and data foundations, with security designed in.

7 Advice with integrity

We recommend only what you need and tell you why, and we take no commission or referral fee from the firms we introduce, so our advice serves you alone.

8 A roadmap

You know what comes next, and what it will cost, before you decide.

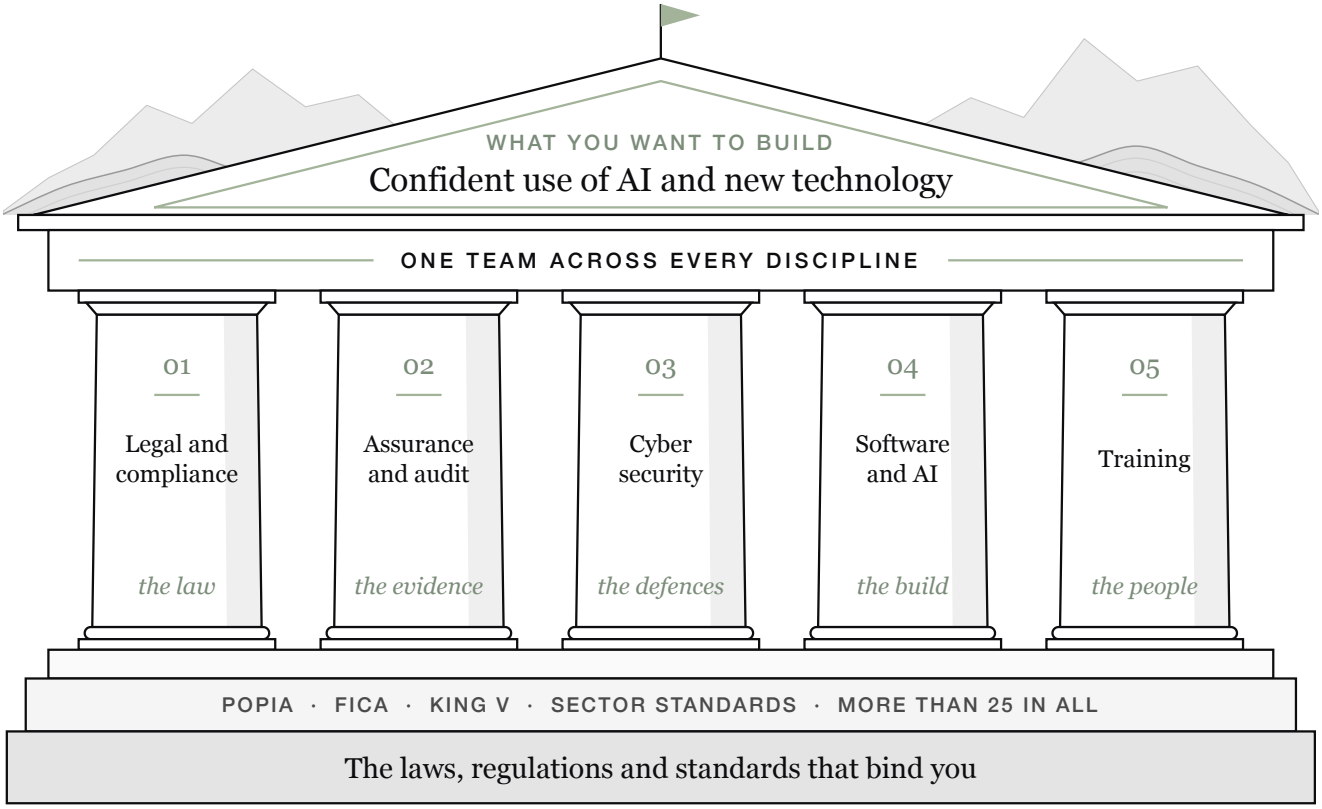


What we bring

What you build with AI needs every pillar standing.

Artificial intelligence can change how your business works, and regulation follows close behind. A single tool that reads your customers' documents touches data protection law, the controls an auditor will test, the routes an attacker might try, the way the system is built and the people who use it. In South Africa the rules for AI are largely the ones you already live by, from POPIA and King V to your sector's standards, applied to new tools.

So we believe that to make the best use of AI, and to keep what you build within the rules, you need a team that knows all five domains modern regulation covers. Our practice leads come from regulatory, audit and in-house backgrounds. Among us are legally qualified consultants, chartered accountants, IT auditors, certified ethical hackers and AI-first developers, all working from one plan.



We set out the laws and contracts your AI and data touch, in plain words, and track the changes that reach you.

We turn your policies and controls into evidence, ready before the auditors ask, and follow every finding until it closes.

We test your systems and AI tools as an attacker would, with a plan and a team to call on for an incident.

We build working systems, AI automations and data foundations with security designed in, and deploy JARVIS into your business.

We teach your people what their work asks of them, from AI guardrails to privacy, with proof that each person completed it.

Your sherpas

The people you will work with.

DIRECTORS



Wessel Swanepoel

Cyber security, resilience and technology risk, and the engineering of our own platforms. More than fifteen years in information and communication technology, with oversight of our security testing and incident response.

BSc Honours in Business Information Technology · Certified Ethical Hacker (CEH)

LinkedIn



Ruan Dickinson

Legal, compliance and intellectual property. SOC 2 readiness and information security governance, and governance and compliance for healthcare practices. More than a decade in intellectual property law.

LLB, University of Pretoria · Qualified trade mark practitioner

LinkedIn



Stefan Oberholzer

Legal, regulatory and compliance advisory in technology-driven businesses, with a focus on financial services and insurance. More than ten years as an ICT legal and compliance specialist, building compliance into enterprise risk management.

LLB

Your sherpas

More of the people you will work with.

HEADS OF PRACTICE



Heike van Beek

LEGAL AND FICA SPECIALIST

FICA compliance, data protection and privacy, and compliance risk management programmes.

BCom Law · LLB

LinkedIn



Greg Da Encarnacao

ASSURANCE LEAD

Financial and IT audit, internal controls, pre-assurance and assurance readiness.

Chartered Accountant, CA(SA)

LinkedIn



Shaune Beyleveldt

HEAD OF CYBER SECURITY AND AI-FIRST DEVELOPMENT

Resilience, disaster recovery and incident response planning. More than ten years in IT operations and security implementation.

Higher National Diploma, Computer Science

LinkedIn



Charlie Cloete

HEAD OF INTERNAL PRODUCT DEVELOPMENT

JARVIS, and secure development across the software development lifecycle (SDLC). .NET, Dataverse, Power Platform and DevOps.

BEng (Hons) Computers

LinkedIn



Emma Lockwood

TRAINING AND SOFTWARE IMPLEMENTATION

Training, implementation and support: our learning platform, JARVIS and client data.

BA · LLB, University of Pretoria

LinkedIn



Janie Venter

LEGAL AND PRIVACY SPECIALIST

Compliance advisory, POPIA and FICA, and legal and compliance documents. Certified mediator.

BCom Law · LLB

LinkedIn



Arista Mootheram

LEGAL AND COMPANY SECRETARIAL SPECIALIST

Labour law, workplace governance and HR compliance.

BA Law · LLB

LinkedIn



Carla Walkenshaw

GOVERNANCE AND AUDIT SPECIALIST

Audit readiness, technology risk, and disaster recovery and resilience testing. A big four IT audit background.

BCom Honours in Internal Auditing

LinkedIn



Sonja van der Merwe

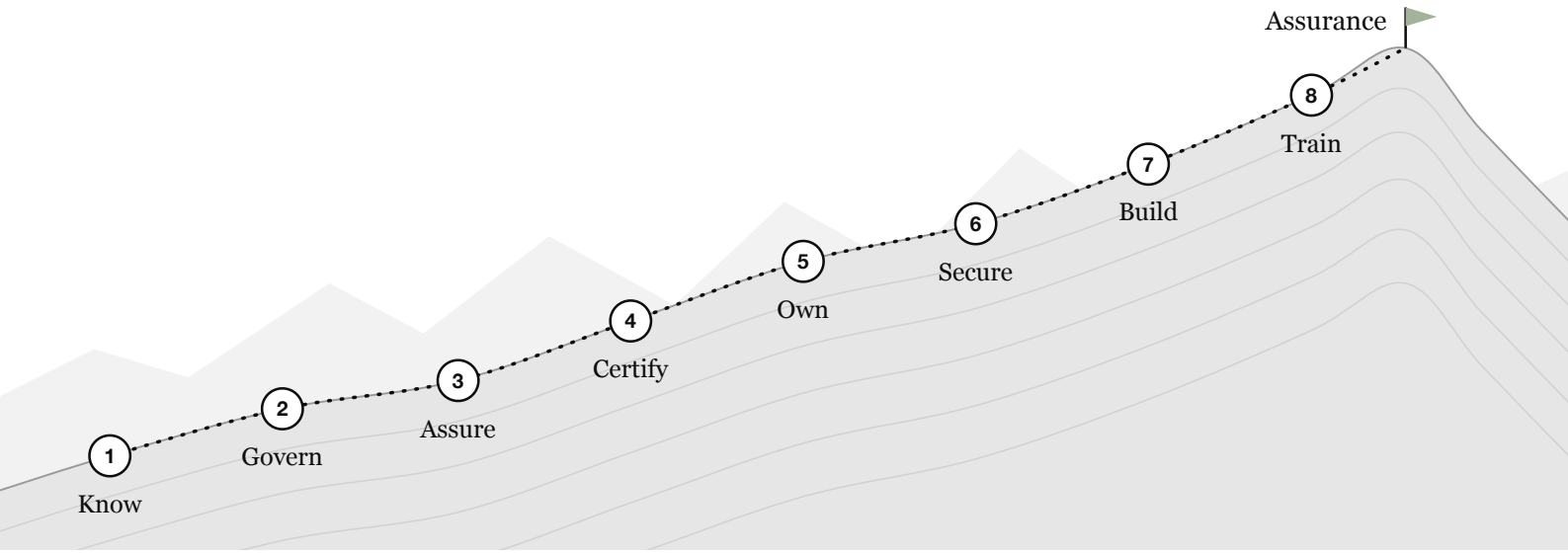
TRAINING

Training development and rollout, with completion evidence on our learning platform.

The route

One route. Eight steps.

Each step answers a question your board already asks. The steps run from knowing what binds you to teaching your people what changed. You can join at any step, and we will show you what comes before and after it.



1 Know

What must we comply with?

Know the laws, regulations and contracts that bind you, in plain words, with an owner and a control for each.

2 Govern

Who decides, and by what rules?

Written policies and ready plans for technology, AI and risk, and a board that knows which decisions are its own.

3 Assure

Can we prove it?

Audit evidence gathered in advance, each finding tracked to its close, and answers your customers and insurers can check.

4 Certify

What will the auditor ask of us?

We prepare you for ISO/IEC 27001, SOC 2 and PCI DSS and sit in with the auditor. The certificate or report is theirs.

5 Own

Do we own what we have built, and can we keep what we rely on?

Know what you own, hold the agreements that prove it, and have a plan to keep using the software you rely on if its supplier fails.

6 Secure

Would we withstand an attack, and cope with one?

We test your defences as an attacker would, and give you a plan and an incident manager to call on when an incident comes.

7 Build

Do we have the software and AI our business needs?

Data foundations, AI automations and software, with security designed in.

8 Train

Do our people know what to do?

We teach your people what the first seven steps decided and built, and keep the completion reports that show they were taught.

Where to start

Start with what is pressing.

Six pressures bring organisations to us. Each has a natural first step, and every first step leads onto the route.

The regulator

You must show what binds you, and who owns each duty.

START WITH

A map of the laws and duties that apply to you, in plain words, each with an owner and a control. It covers POPIA, PAIA and FICA where they apply and, for financial institutions, the Joint Standards on IT governance and on cyber security and resilience.

ON THE ROUTE

1 Know

The auditors

Auditors want evidence, not intentions.

START WITH

A readiness review, packs of evidence for the auditor, and one tracker that follows each finding to its close.

ON THE ROUTE

3 Assure

Customers and insurers

The security questionnaire arrives before the contract does.

START WITH

The questionnaire in front of you, or a gap assessment against the standard your customers name: ISO/IEC 27001 for information security, SOC 2 for service providers or PCI DSS for card payments.

ON THE ROUTE

3 Assure · 4 Certify

Attackers

Your systems are being tested, whether you test them or not.

START WITH

A penetration test, and an incident response plan with playbooks for ransomware and phishing, which your team rehearses before you need it.

ON THE ROUTE

2 Govern · 3 Assure · 6 Secure

AI

The King V governance code asks boards to account for data and technology, AI included, and your people already use AI without written rules.

START WITH

An AI Governance Review and an AI policy, or a data and AI readiness review if you want to build.

ON THE ROUTE

2 Govern · 7 Build

Too many advisers

Each adviser sees only their part, and the gaps between them are yours.

START WITH

One roadmap under one named lead: the Managed Compliance Function or the Outsourced CISO.

ON THE ROUTE

1 Know · 2 Govern · 3 Assure · 6 Secure

Who we work with

Organisations like yours.

We work for organisations of many kinds. Below is what each kind most often comes to us for. We name no client here.

KIND OF ORGANISATION	MOST OFTEN COMES TO US FOR	ON THE ROUTE
Insurers Bound by the Joint Standards on IT governance and cyber security, with boards asking about King V and AI.	Privacy, the financial sector standards, IT and AI governance, audit support and assurance, and software we build for them.	1 Know · 2 Govern · 3 Assure · 7 Build
Financial services and credit providers FICA and FAIS duties where they apply, credit law and the financial sector standards, with compliance officers of their own.	FICA and FAIS, credit law, the financial sector standards, privacy, company secretarial work, governance, incident response and training.	1 Know · 2 Govern · 6 Secure · 8 Train
Property groups FICA duties as property practitioners, and the personal information of tenants and buyers.	FICA, privacy, a map of the laws that bind them, and training on our learning platform.	1 Know · 8 Train
Manufacturers and industrial groups Large workforces and groups of companies, each with its own laws to keep.	Compliance training for their people, privacy, FICA, corporate governance and enterprise risk, employment law and IT governance.	1 Know · 2 Govern · 8 Train
Medical schemes and healthcare practices Health information is special personal information under POPIA.	Privacy, contracts and employment law, AI and corporate governance, modules on JARVIS and training.	1 Know · 2 Govern · 7 Build · 8 Train
Technology and software companies A contract with every customer, and customers who ask for evidence of security.	Commercial legal advice and contract review, privacy, employment law, IT governance, and audit support and assurance.	1 Know · 2 Govern · 3 Assure
Engineering and consulting firms Project and sub-consultancy contracts, and the personal information of clients and staff.	Privacy, contract review, FICA, incident response and training.	1 Know · 6 Secure · 8 Train
Accounting and professional practices Some carry FICA duties, and client confidentiality sits at the core of the work.	FICA, privacy, company secretarial work, trade mark searches, IT governance, modules on JARVIS and training.	1 Know · 2 Govern · 5 Own · 7 Build · 8 Train
Industry bodies and membership organisations Member data, governance that answers to members, and training for their industry.	Privacy, company secretarial work and corporate governance, contracts and disputes, software and modules on JARVIS, and training for their members.	1 Know · 2 Govern · 7 Build · 8 Train
Agricultural businesses Supplier and buyer contracts, and the personal information of workers.	Privacy, FICA, contract review and training on our learning platform.	1 Know · 8 Train

Featured solutions

Six solutions, one named lead each.

Each draws services from the route under one plan and a price agreed before we start. A review or a project has one fixed price; a function we run for you has a fixed monthly fee for a year, renewed with the roadmap for the year ahead.

Outsourced CISO

A chief information security officer (CISO), without the full-time hire

ON THE ROUTE

1 Know · 2 Govern · 3 Assure · 4 Certify · 6 Secure · 8 Train

Your security has one named lead, a yearly plan and a monthly record.

A named lead and our specialists run your security programme for a fixed monthly fee, with no full-time appointment to make.

- Leadership and reporting
- Legal obligations and suppliers
- Governance, risk and policy
- Customer and insurer assurance
- Technical security and oversight of testing
- Incident readiness
- Secure development and AI use
- Awareness training

FICA Suite

For businesses bound by FICA, the anti-money-laundering law

ON THE ROUTE

1 Know · 7 Build · 8 Train

A FICA programme ready to approve, and customers screened and monitored.

Your FICA duties, written down and kept current. We build the risk assessment and programme for your approval, prepare your compliance officer's appointment, bring your existing customers up to date, then monitor them every month. Your compliance officer keeps the role, you approve the programme and file the reports, and we do the groundwork.

- Risk assessment and programme
- Compliance officer appointment
- Due diligence procedures
- Screening and risk rating
- Employee screening
- Return preparation and inspection support
- Training for staff and board
- A programme kept current each year

Managed Compliance Function

Your compliance function, run with you

ON THE ROUTE

1 Know · 2 Govern · 3 Assure · 8 Train

You keep the role. We run the compliance function behind it.

Under a named lead and a roadmap you have adopted, we keep your compliance register, policies, contracts, risks and training current month by month. You receive one invoice with an extract of the work completed, so you know what was done.

- Compliance universe
- Governance and risk
- Privacy and PAIA upkeep
- Contract desk
- Employment documents
- Legal Compliance Support
- Findings tracking
- Yearly training programme

Featured solutions, continued

Three more solutions, on the same terms.

Incident Response

Before, during and after an incident

ON THE ROUTE

1 Know · 2 Govern · 6 Secure

When an incident comes, the plan is written and the manager is named.

We prepare you first, with an incident response plan, a disaster recovery plan and a simulation in which your team rehearses them while we observe. When an incident comes, an incident manager runs the response and supports your communication with customers, insurers and the board. We prepare the notifications the law requires, to the Information Regulator and the people affected, for you to send. Afterwards you hold a forensic report, a close-out pack and a hardening roadmap.

- Incident plan and playbooks
- Planned and observed exercises
- Standby or built-in first response
- An incident manager
- Notifications the law requires
- Customers, insurers and board
- Final report and close-out
- When the regulator asks

Software Development

Security, governance and ethical AI first

ON THE ROUTE

1 Know · 2 Govern · 3 Assure · 4 Certify · 5 Own · 6 Secure · 7 Build

Software and AI automations with security and governance built in, tested before go-live.

We build AI automations, AI-powered software and AI skills and procedures, with security, privacy, governance and ethical AI designed in from the first specification. Our compliance consultants write the rules into the specification before the first line of code. Before go-live, another of our consultants, who did not build it, reviews and tests it, and our developers fix what is found.

- Data and AI readiness
- AI automations
- AI-powered software
- AI skills and procedures
- Modules on JARVIS
- Privacy and security by design
- The auditor's document set
- Run and support

Pen-Testing

Ethical, audit-ready, actionable

ON THE ROUTE

6 Secure

Find what an attacker could reach, with a recommended fix for each finding.

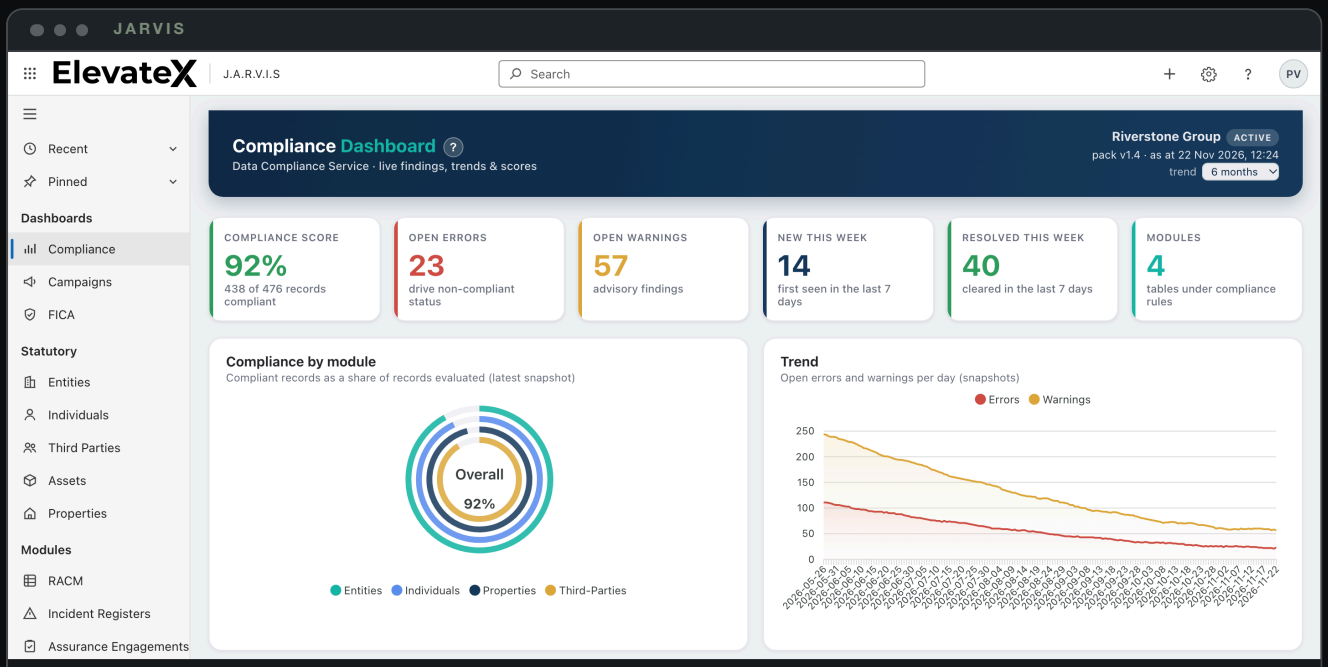
We test the systems you run and report each finding by what we showed an attacker could do, with its evidence and a fix. Then we retest what you have fixed, and give you a closure report and a letter you may show your customers and auditors. Our cyber security practice does the testing, and a Certified Ethical Hacker oversees it.

- Authorisation and test plan
- Sixteen kinds of test to choose from
- Critical findings reported during the test
- A report you can act on
- Remediation workshop and retest
- Tester's letter
- Cyber Assurance Subscription

Our products · JARVIS

One secure record of your entities, people, third parties and obligations.

JARVIS is our compliance platform, built on Microsoft Power Platform. It keeps each entity, person and third party in one place with its documents and history, and checks the records against the rules we set up with you every hour. Your team works in JARVIS, and the outside parties you deal with answer through a secure portal that carries your brand.



The compliance dashboard, with every module in the menu beside it: the score by module and the trend in open errors and warnings. Fictitious data.

Company secretarial

Entities, directors, shareholding and statutory documents, with the group organogram drawn from the share records.

Third parties

Suppliers, brokers, members and partners, each with its contacts, documents and the rules for its type.

Campaigns

Each designed for its purpose: who it goes to, what it asks, when it reminds and who checks the answers.

Policies

Each policy and procedure from draft through review and approval to its published version.

Risk and incidents

Risk registers with controls and owner reviews, and a register of privacy incidents.

Assets and properties

Vehicles, IT assets, trade marks and properties, with owners, leases and insurance.

FICA

Customer due diligence, employee screening and monitoring once a file is complete.

Reporting and AI

Live dashboards, scheduled reports, registers and Excel exports, and AI that reads FICA documents.

YOUR TENANT, OR OURS

Your records sit in a Microsoft Dataverse environment in your own tenant or one we manage, under Microsoft sign-in. The portal and the automation run as a service we host.

SHAPED TO YOUR BUSINESS

Your own fields, forms and views sit beside a shared core that we keep up to date, and we build new modules on the same platform.

ACCESS AND HISTORY

Access is set by role, down to single columns, and changes to the records we audit are kept with who made them and when.

We host and process your data in compliance with the regulatory and contractual requirements that apply to it.

JARVIS · Company secretarial

Every entity, director and share, and the group structure drawn from them.

One profile for each company, trust and partnership in your group, and one for each person, whatever roles they hold. The organogram and the beneficial ownership register come from the same share records.

Entity profiles

Type, status, registration and tax numbers, year end, auditor, company secretary and information officer.

Principals

One profile per person, with every appointment and resignation as director or trustee, and every holding, kept as history.

Shareholding

Share classes and certificate details, and every allotment, transfer, buy-back and cancellation with the documents behind it.

Group organogram

Drawn from the current share records each time it opens, by ownership or investment, with foreign and circular holdings shown.

Beneficial ownership register

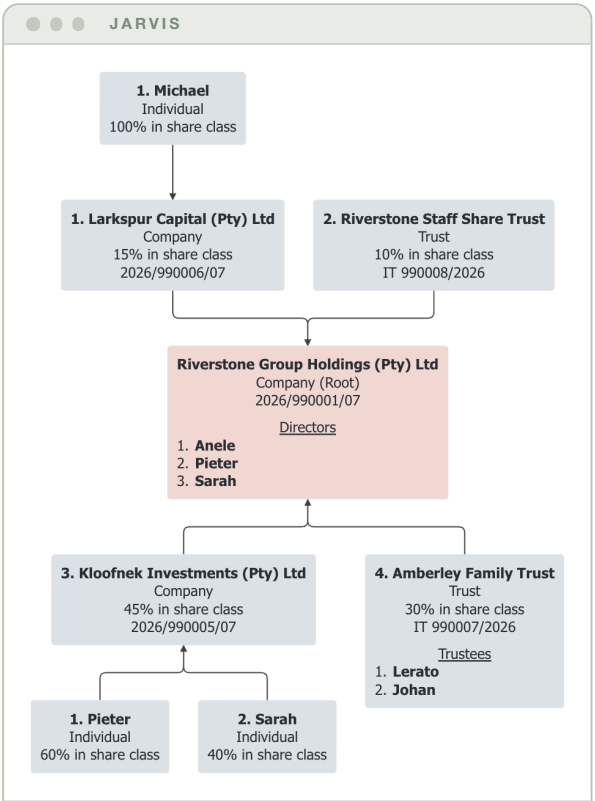
One workbook of the natural persons above your threshold, with the workings and each chain, for your designated person to file.

Statutory documents

Resolutions, minutes, the MOI and CIPC forms kept by register against each entity, with rules we set up that flag what is missing.

Dashboards

A compliance score by module, open findings, and the records that need attention.



The group organogram, drawn from the share records: each arrow runs from a shareholder to the company whose shares it holds. Fictitious data.

COMMON COMPANY SECRETARIAL PROBLEMS, AND HOW JARVIS HELPS

THE PROBLEM	HOW JARVIS HELPS
The securities register falls behind the share transactions (Companies Act 71 of 2008, s 50).	Each allotment, transfer and cancellation is recorded against the certificate it affects, with its document.
Beneficial ownership is not filed with the CIPC, or not kept current (s 56(7)).	The register is worked out from the share records, with the workings, for your designated person to file.
Annual returns are filed late (s 33 and regulation 30).	Each private company carries its last and next annual return dates, and a missing CoR30.1 can be flagged.
Changes of directors are not lodged on CoR39 within 10 business days (s 70(6)).	Each appointment and resignation carries the date the CIPC was advised, and a missing CoR39 can be flagged.
Past directors drop off the register (s 24).	A resigned director stays on record with the date and the reason.
A trust's beneficial owners are not lodged with the Master (Trust Property Control Act s 11A).	Trustees and beneficiaries are recorded, and the ownership calculation looks through each trust to the people behind it.

JARVIS · Third parties

Know every third party, and collect what you need from them without chasing.

Each third party has one profile, with its contacts, its link to your entities and its documents. When you need information from many of them at once, a campaign designed for the purpose picks out the right parties, sends each a request in your brand, follows up on schedule and checks what comes back.

Third-party profiles

Type and subtype, registration, VAT and tax numbers, addresses and contacts, and how each party relates to your entities.

Rules for each type

Required documents, expiry dates and data checks, which we set per type, so a broker, a supplier and a member are each held to their own standard.

Information request campaigns

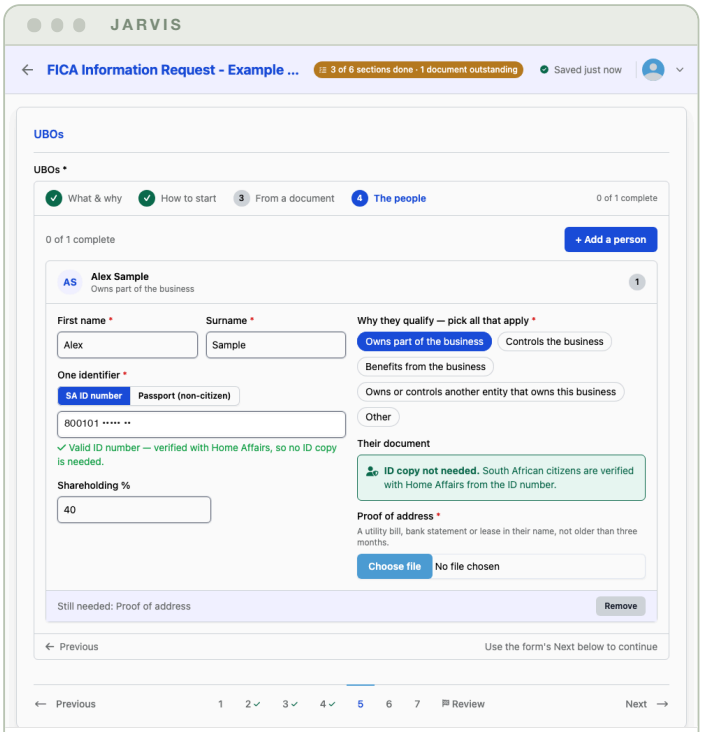
Each campaign picks its parties by rules on your records, such as a type or an expiring document, with its own form, due date and reminders.

Answers checked before they land

You choose which answers wait for a reviewer, who sees the old and the new value and approves or declines each change.

Documents and agreements

Documents received are filed against the party with their dates, and the rules we set up flag missing or expired ones.



A request in the portal, captured step by step, with checks as the answers go in. Fictitious data.

CAMPAIGNS WE HAVE DESIGNED

CAMPAIGN	WHAT IT MEETS
FICA due diligence	Customer due diligence under the FIC Act, beneficial owners included.
Risk register review	Each owner confirms their risks and controls on a set cycle, as evidence for the board.
Member information update	An industry body's member register and voting rights kept current.
Vendor compliance review	Supplier details and compliance documents brought up to date.
Franchise cyber security assessment	Assurance that franchisees protect the personal information they handle.
Professional indemnity cover	An insurer's check on intermediaries' cover, sent only to those whose cover is missing or about to expire.

Because each campaign is designed rather than built, the same engine carries other questionnaires, such as supplier privacy and security reviews.

JARVIS · On the same platform

Policies, risks, assets and FICA, run by the same engines.

Each policy, risk, property and FICA file stays with the record it belongs to, and every module draws on the same engines.

ON THE SAME RECORDS

Policies and procedures

Each controlled document moves from planned to draft, review, approval and finalised, with each responsible group asked in turn: drafted in Word from the portal, approved on a shared PDF with annotations and published to a SharePoint library or your intranet.

Risk, incidents and findings

Risk registers sit in legal categories with controls and owners, and owner reviews run as a campaign with reports by entity and for the group. Privacy incidents are recorded with their impact, timeline and the Information Regulator's case status, and assurance findings are followed to closure.

Assets and properties

You keep one register for vehicles, equipment, IT assets and trade marks, with values, insurer and policy, and a profile for each property with its erf and title deed, valuation, each owner with its percentage, leases and insurance.

FICA

Customer due diligence and employee screening run on the same records: identity is checked with Home Affairs and company details with the CIPC, a consultant decides each sanctions, PEP or adverse media hit, and a complete file is re-screened monthly against the UN sanctions list. The FICA Suite among our featured solutions runs on JARVIS.

THE ENGINES BEHIND EVERY MODULE

Hourly compliance checks

Every hour a rule engine checks your entities, people, third parties and properties against the rules we set up with you, for missing fields and documents, expired details, invalid values such as South African ID numbers, and duplicates. Each record gets a status and the reason for it, and your dashboard gives a score by module and the records that need attention.

Workflows and approvals

Processes run in ordered and parallel steps, with due dates, approval gates decided by the people you name and conditions that skip what does not apply. Automations run when a record changes as well as on a schedule, a step can produce a Word or PDF document from the record, and a timeline shows every step, who acted and when.

Forms and questionnaires

Forms are set up as data, not code, with pages, repeating tables and about twenty kinds of field. Answers are checked as they go in, respondents can stop and come back, each document is read as it arrives, with advice on whether it is the right kind and current, and every form carries your brand.

Committees and board packs

You run committees with their members, meetings and papers. When a meeting's invitation date arrives, each member receives the papers in the portal and marks each one read, and weighted votes produce an outcome workbook.

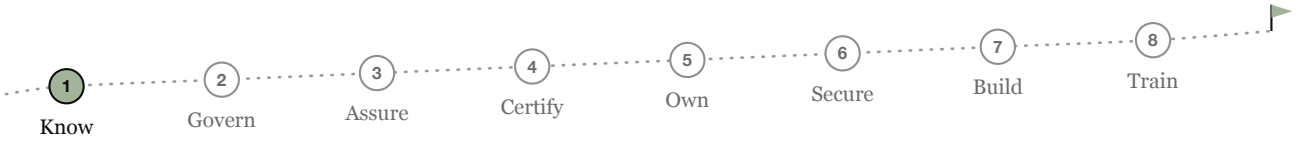
Campaigns designed for each purpose

Each campaign is designed for its purpose: who it goes to, chosen by rules on your records, what they are asked, and when and how often they are reminded. Respondents need no account or password, and you see completion, time to complete and who to chase.

Reports and dashboards

Every module reports from the same records: dashboards shown only to those who may see them, scheduled reports in your inbox, and report pages with CSV export and print to PDF. Statutory registers are built for you, beside the beneficial ownership workbook, Excel from every view and Power BI connected to the same data.

STEP 1 OF 8 ON THE ROUTE



1 The regulatory and compliance universe

KNOW

Know what binds you, duty by duty.

What must we comply with?

We list every law, regulation, standard and contract that binds your business, from POPIA to the rules that reach your use of AI, and set out each duty in plain words, with a rating, an owner and a control. Then you know what you must comply with, and what to fix first.

WHAT WE DO

- **Your compliance universe.** We decide which laws, codes, standards and contract terms apply to each of your entities, and score where you stand against each.
- **Privacy under POPIA and PAIA.** We assess each department against POPIA, map the personal information it handles, and prepare what your Information Officer files with the Information Regulator.
- **FICA and your sector's rules.** We write your FICA programme, onboard customers on our screening service, and work through FAIS, credit law and the Joint Standards where they apply.
- **Contracts, people and company records.** We review the agreements you sign, draft your employment documents, correct your company registers and CIPC filings, and prepare your answers to regulators.

WHAT YOU HOLD

- A regulatory universe workbook, every obligation rated and owned
- A compliance risk register and a roadmap by quarter
- Your privacy policy, notices and PAIA manual (how records are requested)
- A record of processing: the personal information each department handles
- Your FICA Risk Management and Compliance Programme, ready for your approval

SERVICES

Compliance universe · Privacy compliance · Company secretarial · FICA (anti-money laundering) · FAIS (financial advice) · Financial sector standards · AI regulation · Commercial legal advice, drafting and restructuring · Contract review · Other statutes (such as credit, consumer protection and competition law) · Employment law · Disputes and regulator engagement

12 SERVICES · 85 WORK PACKAGES

WHY ELEVATEX

1

Legally qualified leads

Legally qualified people lead our legal, managed compliance and FICA practices, so the laws that bind you are read by those trained in them.

2

Kept current as law changes

We track the changes in law that touch your business and alert the owners concerned by e-mail from JARVIS, our compliance platform.

3

Privacy for every sector

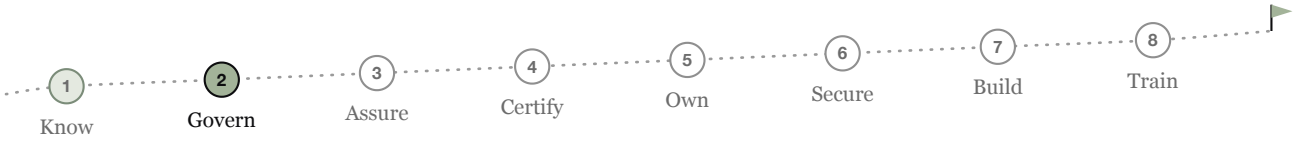
Organisations of every kind, from insurers to agricultural businesses, come to us for privacy work under POPIA and PAIA.

THE STARTING POINT

Every later step starts from your regulatory universe workbook: step 2 writes the policies it calls for, step 7 makes it a live register on JARVIS, and step 8 plans the year's training from the laws it names.

NEXT ON THE ROUTE 2 **GOVERN**

Step 2, Govern, turns the obligations in your regulatory universe workbook into decisions: the policies, plans and committees that say who answers for each.



2 Governance

GOVERN

Name who decides, and put the rules in writing.

Who decides, and by what rules?

Your board answers for every decision taken in its name, from spending limits to the use of AI. We help you put it in writing: who decides on spending, risk, technology and AI, under which policies, and with which plans ready for a bad day, each settled with its owner and adopted by your board.

WHAT WE DO

- **Settle who decides what.** We draft your governance framework, committee charters and delegation of authority, so it is clear which body decides what, and up to which value.
- **Rules and accountability for AI.** We write the rules for your systems, data and AI tools, register the AI you use, and set up the forum that approves it.
- **When something goes wrong.** We prepare an incident response plan with ransomware and phishing playbooks, and a disaster recovery plan with recovery targets your business has agreed.
- **Risks your board can see.** We build your enterprise and IT risk registers, with an owner for each risk, on JARVIS or as workbooks.

WHAT YOU HOLD

- Information security and acceptable use policies, with rules for AI
- An AI policy and responsible AI principles, ready to adopt
- Incident response and disaster recovery plans, issued for signature
- IT and enterprise risk registers, on JARVIS or as workbooks
- Committee charters, packs and signed minutes

SERVICES

IT governance · AI governance · Corporate governance and enterprise risk

3 SERVICES · 34 WORK PACKAGES

WHY ELEVATEX

1

Drafted to your codes

Our IT governance and managed compliance practices draft against the King code your board applies, and map a financial institution's framework to the Joint Standards.

2

Group rules, local law

For a subsidiary of a group, we compare the parent's global directives with South African law clause by clause, and record each gap.

3

Never from a blank page

We draft from our master documents in your names, systems and corporate identity, or mark up your own policy where it already works.

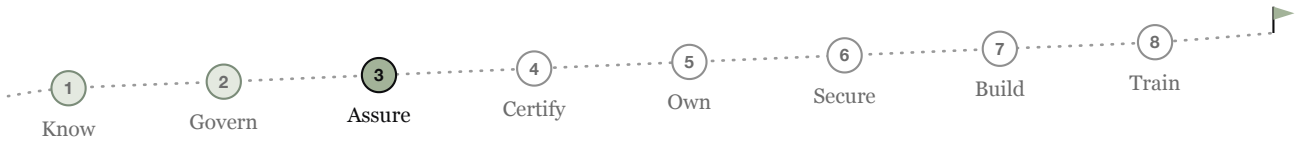
BUILDS ON STEP 1

Your regulatory universe workbook from step 1 names the laws your framework, charters and policies must answer, and your AI policy refers to the privacy policy written there.

NEXT ON THE ROUTE 3 **ASSURE**

Step 3, Assure, readies the evidence your auditors, customers and insurers will ask for, including proof that these plans work.

STEP 3 OF 8 ON THE ROUTE



3 ASSURE

Assurance and audit

Prove what you do, before anyone asks.

Can we prove it?

This is where your policies and plans meet the people who check them: your auditors, customers and insurers. We gather the evidence each of them asks for, so that when the questions come, your answers stand on proof.

WHAT WE DO

- **Beside you at the audit.** We prepare your evidence before fieldwork, then sit beside your auditors, explaining their questions to your teams and your teams' answers to them.
- **Recovery and incident exercises.** We plan the restore test, recovery simulation and incident exercise your team runs, observe and record each, and draft the report you sign.
- **Assurance through the year.** We set the year's assurance plan, then test your controls and audit your POPIA programme through consultants who did not design them.
- **Answers for customers and insurers.** We draft your answers to security questionnaires and your cyber insurance proposal form, each answer tied to its evidence, for you to submit.

WHAT YOU HOLD

- Evidence packs filed by system and control
- A findings tracker, with a quarterly report to your audit committee
- Signed reports on your recovery and incident exercises
- A library of standing answers, each tied to its evidence
- From the architecture review: a target architecture and a ranked roadmap

SERVICES

Audit support · Internal assurance and findings tracking · Client and insurer assurance · Architecture review

4 SERVICES · 22 WORK PACKAGES

WHY ELEVATEX

1

From the auditor's side

A chartered accountant from financial and IT audit leads our assurance practice, and IT auditors and recovery specialists do the work beside you.

2

One tracker, every source

Every finding, whatever its source, goes into one tracker with an owner and a date, and is followed until it closes.

3

Consistent answers

Each answer you give comes from a library we keep current, so it stays consistent from one questionnaire to the next.

BUILDS ON EARLIER STEPS

The regulatory universe workbook from step 1 gives each duty an owner and a control to test. Your policies and plans from step 2 are put to the test here.

NEXT ON THE ROUTE 4 **CERTIFY**

When an outside body is to confirm your controls, step 4, Certify, prepares you for its audit from the evidence gathered here.



4

CERTIFY

Framework implementation

Ready for the standard your customers name.

What will the auditor ask of us?

Whether your customers ask for ISO/IEC 27001, a SOC 2 report or PCI DSS, we take you from the gap assessment to the audit, with the scope, risks, policies and evidence the framework asks for. The certificate or report is the outside body's to give, and we sit beside you while the auditor works.

WHAT WE DO

- **ISO/IEC 27001 from gap to audit.** We assess the gaps, agree the scope, run the risk workshops behind your Statement of Applicability, and sit in at both audit stages.
- **SOC 2 and SOC 1 reports.** We set out your controls with their owners, mapped to the trust services criteria, then keep evidence coming through the Type 2 period.
- **PCI DSS for card payments.** We map where cardholder data flows and which version 4.0.1 requirements apply, then prepare the self-assessment you sign each year.
- **Your AI against ISO/IEC 42001.** We measure your AI governance against ISO/IEC 42001 inside the AI Governance Review, and give you a written position and a roadmap.

WHAT YOU HOLD

- A gap assessment and a dated roadmap, before you commit
- An ISO/IEC 27001 Statement of Applicability and risk treatment plan
- SOC 2 risk and control matrices and a system description
- A PCI DSS self-assessment and attestation for your signature
- An evidence library, filed control by control

SERVICES

ISO/IEC 27001 · SOC 2 and SOC 1 · PCI DSS · ISO/IEC 42001 gap assessment

4 SERVICES · 18 WORK PACKAGES

WHY ELEVATEX

1

Only the real gaps

Our IT governance, risk and compliance practice maps a framework you already hold to the next, so only the real gaps remain.

2

Your management briefed

We brief your top management on the questions an auditor is likely to ask, and agree our seat in the room beforehand.

3

Beyond the first audit

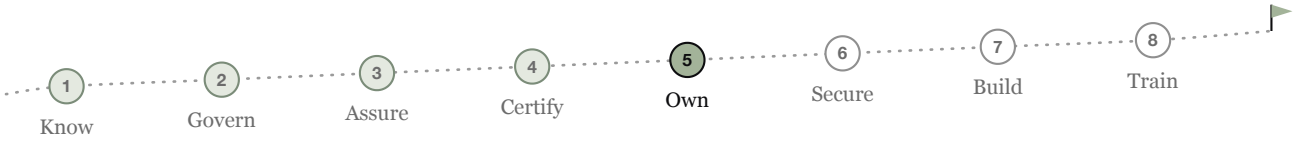
After the first certificate or report, we prepare each surveillance audit, the next SOC 2 period or the yearly PCI DSS self-assessment with you.

BUILDS ON EARLIER STEPS

Your information security and acceptable use policies from step 2 are revised, not rewritten. The signed reports on your recovery and incident exercises from step 3 become audit evidence, and the ISO/IEC 42001 gap assessment starts from your AI policy.

NEXT ON THE ROUTE 5 **OWN**

With your controls in order, step 5, Own, turns to what you own: your brand, your intellectual property and the software you rely on.



5
OWN

Intellectual property and protections

Own what you paid for.

Do we own what we have built, and can we keep what we rely on?

Paying someone to build your software or design your logo does not always make it yours. We show you what you own, draft the agreements that record it, search your trade marks before they are filed, and give you a plan to redeploy the software you rely on if its supplier fails.

WHAT WE DO

- **Trade marks, searched and planned.** We search the register and the market, give you an opinion class by class, and plan the filing for the independent firm you instruct.
- **Ownership put in writing.** We review what you hold, find work made by others with no assignment, and draft the assignments, licences and clauses that close each gap.
- **Who owns the code.** We establish who owns a platform a developer built for you, and set out who owns code and content made with AI.
- **If your supplier fails.** We draft or review your escrow agreement and write the plan a new developer would follow to redeploy the software.

WHAT YOU HOLD

- A trade mark opinion and a filing plan by class
- An intellectual property review: what is protected, what is not
- Copyright assignments and licences, ready to sign
- An escrow agreement and a technical redeployment plan
- A register and renewal diary for your marks and domains

SERVICES

Trade mark searches and portfolio · IP advice · Software escrow

3 SERVICES · 14 WORK PACKAGES

WHY ELEVATEX

1

Qualified, with no commission

A qualified trade mark practitioner leads our legal and intellectual property practice, and we take no commission or referral fee on any filing.

2

Developers in the same firm

We build and run our own platforms. We draw yours layer by layer, from the developer's baseline to your customisations, and show who owns each.

3

We can hold the deposit

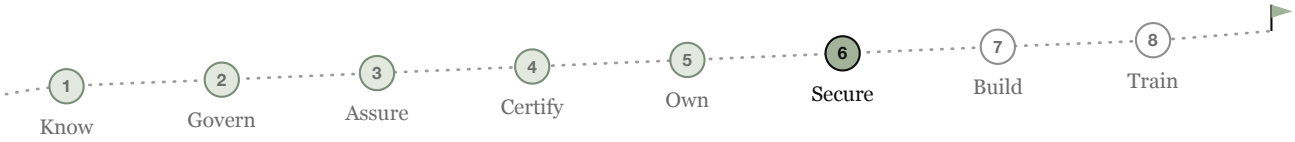
We can also act as your escrow agent and hold the deposit, beside the agreement we drafted and the redeployment plan we wrote.

BUILDS ON EARLIER STEPS

Your intellectual property review starts from the contracts in your regulatory universe workbook from step 1 and from your step 2 AI policy, for work made with AI. The technical redeployment plan sits beside your disaster recovery plan.

NEXT ON THE ROUTE 6 SECURE

Step 6, Secure, tests the systems you run and the domains on your register as an attacker would, and stands ready for an incident.



6 Cyber security

SECURE

Test your defences before an attacker does.

Would we withstand an attack, and cope with one?

We show you what an attacker could reach, with a recommended fix for each finding, in a report your executives can read and your technical team can act on. We retest what you fix. If an incident comes, an incident manager of ours runs the response beside your team.

WHAT WE DO

- **Sixteen kinds of test.** We test networks, cloud configuration, Active Directory, and web, mobile and AI applications, under rules of engagement you sign first.
- **From finding to closure.** We agree each finding's fix, owner and date with your team, then retest and confirm in writing which findings are closed.
- **When an incident comes.** We trace the attack, prepare the POPIA notification to the Information Regulator and any Joint Standards report, and help you submit them.
- **The Cyber Assurance Subscription.** We plan the year's tests, scan each month, run phishing rounds with training on our learning platform, and report quarterly to your risk committee.

WHAT YOU HOLD

- A penetration test report, with the attacker's path and evidence
- A closure report and a tester's letter you may show auditors
- A phishing campaign report, with results by department
- An incident standby, agreed before you need it
- A forensic report and a close-out pack for banks and customers

SERVICES

Penetration testing · Incident response · Continuous assurance

3 SERVICES · 37 WORK PACKAGES

WHY ELEVATEX

1

Certified Ethical Hacker oversight

Our cyber security practice does the work, and a Certified Ethical Hacker oversees our testing and incident response.

2

Findings we proved

We check every candidate finding by hand and rate each on the impact we demonstrated, so your team fixes real weaknesses first.

3

Forensic discipline

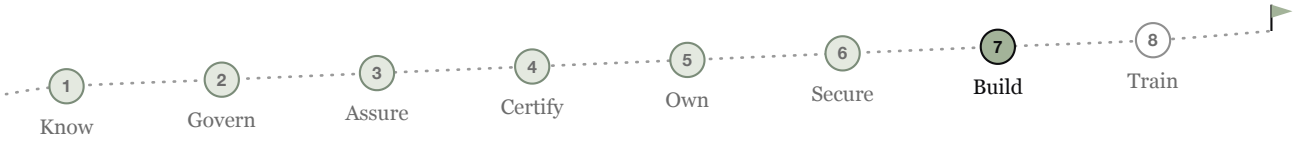
We keep the evidence under chain of custody before anything is rebuilt, and grade each forensic finding as established, inferred or not established.

BUILDS ON EARLIER STEPS

Our incident standby works from your incident response and disaster recovery plans from step 2. A breach is scoped against your record of processing from step 1, and findings map to your ISO/IEC 27001 Statement of Applicability from step 4.

NEXT ON THE ROUTE 7 **BUILD**

Step 7, Build, designs new systems to close the weaknesses your tests found, and another consultant tests each before go-live.



7
BUILD

Software development

Turn your rules into working systems.

Do we have the software and AI our business needs?

This step opens with your data, because a build is only as good as the data beneath it. On that foundation we build the systems that carry your obligations, from compliance registers to AI automations, and look after them once they are live.

WHAT WE DO

- **Data ready for AI.** We map your data and its owners, write the rules that govern it, and build the store your dashboards and AI tools read from.
- **Your registers on JARVIS.** We configure JARVIS modules, load your records, set rule packs that test them, and run campaigns that collect evidence.
- **Built for your processes.** We build the automation, application or AI skills a process needs, and connect it to the systems you already run.
- **After go-live.** We host your system in your cloud tenant or ours, back it up, support it and keep your registers current month by month.

SERVICES

Data and AI readiness · Modules on JARVIS · Bespoke software and AI automation · Run and support

4 SERVICES · 26 WORK PACKAGES

WHAT YOU HOLD

- A data and AI readiness report, with a roadmap
- JARVIS modules, from contracts to FICA customer due diligence
- A first AI use case, measured on your own documents
- Working software or an AI automation, with source code and runbook
- Documents your auditors ask for, with the security test and retest

WHY ELEVATEX

1

Start small, build on it

Our AI-first development and JARVIS teams let you start with a readiness review, one JARVIS module or one process to automate, each scoped in writing first.

2

A platform already built

JARVIS, our compliance platform, already has modules for contracts, policies, third parties and risk registers, so we configure yours rather than build from nothing.

3

Clients we build for

Insurers come to us for software, medical schemes and healthcare practices for JARVIS modules, and industry bodies and membership organisations for both.

BUILDS ON EARLIER STEPS

Your regulatory universe workbook and compliance risk register from step 1 become live registers on JARVIS; your record of processing sets the data rules. Your information security and acceptable use policies and AI policy from step 2 shape each specification.

NEXT ON THE ROUTE 8 TRAIN

Step 8, Train, teaches your people what the earlier steps decided and built, from your policies to the new system.

Step 7 of 8 · Build, in depth

AI and software your board can account for.

Our developers work beside the consultants who read your laws, test your defences and train your people, so your obligations shape a build from its first sketch. You end with a working system, its source code and the record of how it was built and tested.

HOW WE BUILD

1

Understand the work

We read your registers and policies, and sit with the people who run the process before anything is designed.

2

Map and specify

We map the data flows and specify the build: its threat model, its privacy impact and which AI model runs where.

3

Prove the idea

A new idea is first tried on your own data, against answers your people checked, and you decide whether to build.

4

Build and verify

We build in short releases, reviewing and testing the code as it grows, and your process owners sign off each release.

5

Security test and hand-over

Another of our consultants, who did not build it, tests it as an attacker would, and each fix is retested before hand-over.

6

Run and improve

The team that built it fixes any defect in our work as support, and scopes each change before you adopt it.

WHAT WE BUILD

AI automations

For the repeated work in a process: documents read, reconciled with your records and routed to the right person.

Business applications

For the application your business needs, from a member portal to an operations platform, with AI only where it helps.

AI skills and procedures

For tasks like comparing documents: a written, tested procedure, so your people and their AI tools work the same way each time.

AI-ready data foundations

For reporting and AI that stand on data you control: one governed store, access by role, each source recorded.

PROOF IN OUR OWN PLATFORMS

The developers who build for our clients also built JARVIS, our compliance platform; our screening service, for customer due diligence under FICA; and our learning platform, whose completion reports serve as evidence. We run all three for clients.

Ethical AI, written down

We set what each AI feature may decide, where a person approves and what is logged, so its decisions can be traced.

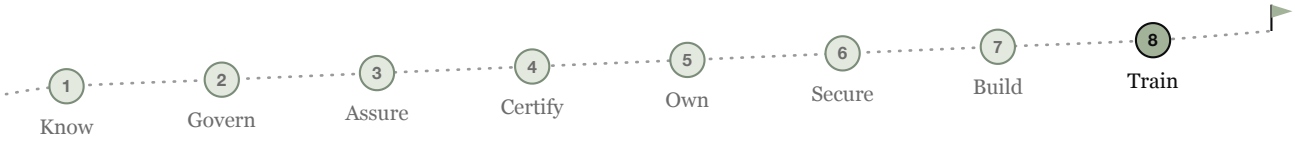
Yours to own and run

Code ownership is agreed in writing before the build, and your administrators are trained to change its rules without a development request.

Benefit you can measure

We measure the process before we build, so after go-live you can see what the build changed.

Our Software Development solution puts security, governance and ethical AI first, from the specification to the system your people run.



8 Training

TRAIN

Teach your people, and keep the proof.

Do our people know what to do?

A policy changes nothing until the people who must follow it know what to do. We teach your staff, managers and board what your policies and systems require of them, and give you the training certificates and completion reports that a regulator or an auditor asks for.

WHAT WE DO

- **Courses for every step.** We write courses on POPIA, FICA, anti-corruption law, cyber security and AI use, adapted to your own policies and sector.
- **On our learning platform.** We enrol your people, open each training window, follow up who is behind, and report completions each month.
- **A training year, planned.** We plan each year's training from your regulatory universe workbook and compliance calendar, inside the Managed Compliance Function or Outsourced CISO.
- **Training an industry's members.** We run an industry body's courses and examinations on a platform in its name, from bulk registration to numbered certificates and grade reports.

WHAT YOU HOLD

- Courses on your own policies, each with a quiz
- A learning site in your branding, with a programme per role
- Training certificates and a final training report for your compliance file
- Completion reports that name who has not yet finished
- A training plan for the year, tied to your compliance calendar

SERVICES

Training content for each step · The learning platform · The yearly training programme · Training for an industry body's members

4 SERVICES · 22 WORK PACKAGES

WHY ELEVATEX

1

Evidence in one place

Our training and support practice runs your courses on our own learning platform, so certificates, completion reports and the training tracker come from one place.

2

All staff to the board

We train every level, from an all-staff POPIA course to Information Officer training and AI briefings for your board.

3

Staff and members alike

Manufacturers and industrial groups, financial services and credit providers, and property groups train their people with us, and industry bodies their members.

BUILDS ON EARLIER STEPS

We build your courses from the earlier steps: the privacy policy, PAIA manual and FICA Risk Management and Compliance Programme of step 1, the AI policy of step 2, step 6's phishing campaign report and what step 7 built.

AND THEN

This is the last step, not the end: when the law changes, we update your regulatory universe workbook, then your policies, then the courses.

ElevateX

Contact us

Navigate complexity.
Achieve assurance.

Book a first conversation. Tell us what is pressing, and we will show you the route from where you stand. Let's summit together.

WHAT HAPPENS NEXT

1

Tell us what is pressing

An audit finding, an incident, a customer's questionnaire, a new law.

2

We map it on the route

In a first conversation we show you where it sits, and what comes before and after it.

3

You receive a scope and a price

A written scope of works: the phases, what you will hold, what we need from you, and the price, before you commit to anything.

TALK TO US

Wessel Swanepoel
Cyber security, technology and software
082 405 8973
wessel@elevatex.tech

Ruan Dickinson
Legal, compliance and intellectual property
072 393 1579
ruan@elevatex.tech

ADDRESS

Park Lane West Building
194 Bancor Avenue, Menlyn Maine
Pretoria, South Africa

REGISTRATION NUMBER

2015/001727/07

VAT NUMBER

4350274058

For your supplier file, ask either of us for the documents your onboarding needs. This edition: November 2026.