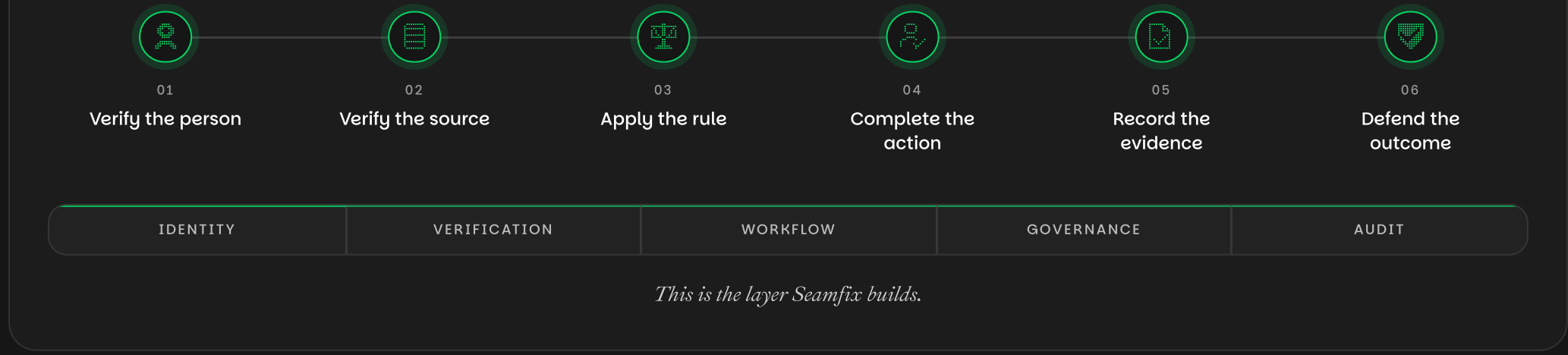
Trust infrastructure for processes that *cannot afford to be wrong.*

Identity, verification and transformation for institutions whose processes must hold up wherever they run.



When trust fails, the process fails.

A citizen cannot access a service.

An account is opened on evidence that cannot be defended.

A subscriber is registered against the wrong identity.

A candidate cannot prove the result is theirs.

A workforce action cannot be attributed to a verified person.

A regulator cannot see whether a control actually ran.

When identity fails, a real person carries the consequence. That is why Seamfix treats identity, workflow and audit as infrastructure rather than interface decoration.

Proven under consequence.

350M+	170+	68+	18+
verified identities	organisations on one governed ecosystem	countries reached by a digital credential service	years of identity-infrastructure delivery

Subscriber-registration remediation delivered inside a 10-day regulatory window.

Seamfix can move identity infrastructure at national scale when a regulator, not the project plan, sets the timetable.

170+ organisations operating on one governed identity ecosystem.

A governed ecosystem can widen participation without the authority surrendering control of policy or evidence.

A sovereign credential service reaching citizens in 68+ countries.

A government can extend a sovereign service internationally without moving authority away from the issuing institution.

One company. Three ways to engage.

Transformation & Consulting

Assess, redesign, implement and operate trust-critical processes.

The Seamfix Platform

A configurable trust-infrastructure core for identity, biometrics, workflow, integration, multi-tenancy and audit.

Fixiam

Verified-person governance for workforce, agents and assessment candidates.

These are not three disconnected businesses. Consulting diagnoses the process. The Platform shortens the route to production. Fixiam governs the human where human assurance is the problem.

The Seamfix Platform.

Current production release: **Platform 9.0**

Platform 10.0 — in programme validation

Layers can be adopted whole or beneath systems you already run.

L1	Experiences	Web · Mobile · Kiosk · Assisted capture · Existing client applications
L2	Programme workflow	Forms · Rules · Review · Exceptions · Approvals · Notifications
L3	Trust services	Identity · Biometrics · Authentication · Source verification · Credentials
L4	Integration	APIs · National sources · Client systems · Third-party services
L5	Governance	Tenant · Role · Policy · Device · Audit · Reporting

Deployment band — programme-approved hosting and residency model

How the Platform is bought.

COMMERCIAL LAYER	WHAT IT COVERS	TYPICAL TREATMENT
Platform licence Recurring	Recurring right to use the agreed Platform deployment and capabilities for the production scope.	Recurring licence under the commercial agreement.
Implementation services One-off or milestone	Discovery, configuration, workflow engineering, integrations, data work, testing, deployment and training.	Fixed, milestone, outcome-based or T&M depending on scope.
Managed operations Optional, recurring	Agreed support, monitoring, DevOps, databases, incident management and continuous improvement.	Optional recurring managed service.
Programme-variable services Variable, disclosed	Approved third-party, cloud, messaging, verification or similar variable services where applicable.	Disclosed in the proposal and contract rather than hidden.

Configure the common controls. Engineer the programme.

WHAT ALREADY EXISTS

- Identity & authentication
- Biometrics
- Capture
- Configurable forms
- Review workflow
- Multi-tenancy
- Device control
- APIs
- Audit
- Credential services

Reuse the trust controls. Engineer the programme.

WHAT BECOMES PROGRAMME-SPECIFIC

- Policy
- User journey
- Integrations
- Data sources
- Rules
- Roles
- Branding
- Operating model

Fixiam: no anonymous actions. No hidden actors.

YOUR EXISTING IDENTITY STACK — STAYS IN PLACE

HR / Directory

- Joiner enrolment
- Leaver revocation

↓

SSO / PAM

- Privileged session

↓

Business apps

- High-value approval
- Sensitive record change

Fixiam

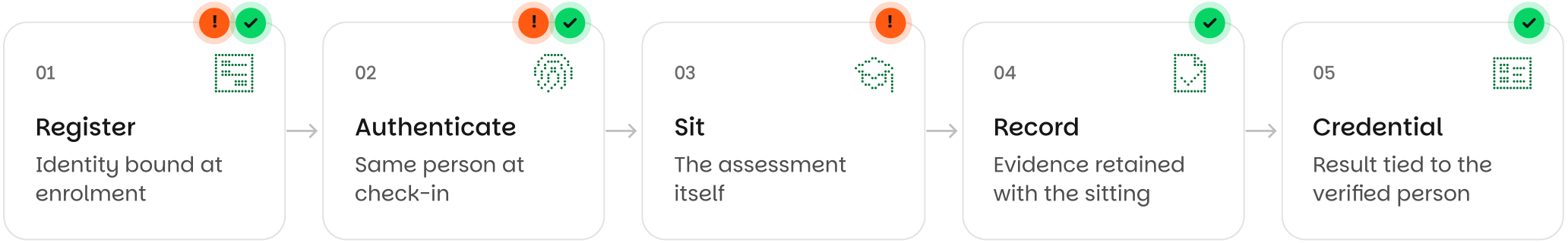
Targeted assurance layer at selected high-risk points

- Verified person
- Biometric assurance
- Lifecycle policy
- Human-bound audit

Keep the identity stack. Add proof of the human where it matters.

Assessment integrity.

Fixiam connects registration, exam access and result evidence to the same verified person without replacing the assessment engine, question bank or scoring system.



Impersonation entry point · Identity re-established

Exception paths remain human-operable.

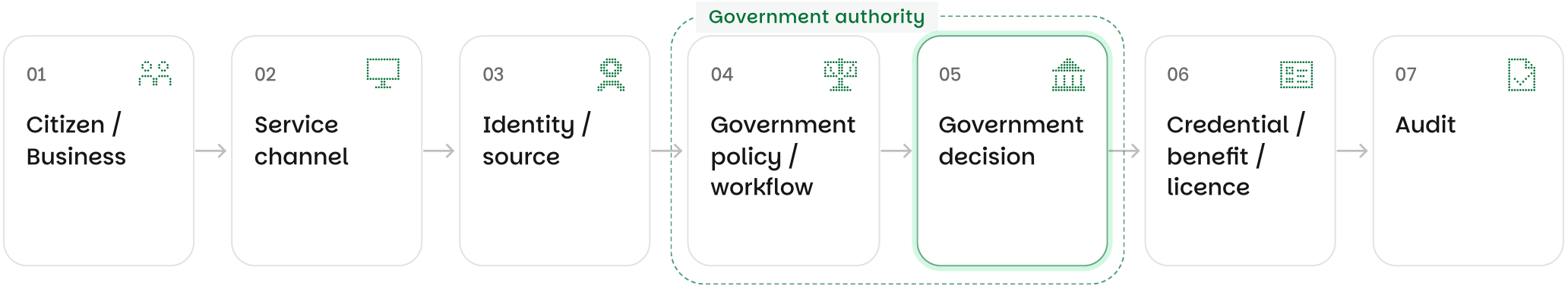
Digital transformation where trust is part of the outcome.

STAGE	YOU RECEIVE	HOW IT IS BOUGHT
01 Assess	Current-state map, control/failure analysis, data & integration inventory, prioritised gaps.	Focused fixed scope; commonly 2–4 weeks.
02 Recommend	Target state, control design, architecture/integration map, privacy requirements, roadmap and costed options.	Fixed or milestone advisory scope.
— You can stop here — the deliverables are yours, even if another supplier implements them.		
03 Implement	Configured service, integrations, data work, testing, training and acceptance evidence.	Milestone, outcome-based or T&M depending on programme.
04 Operate	Support, monitoring, incident/problem management, DevOps/database operations, service reporting and continuous improvement.	Optional recurring managed service.

Telecom trust: subscriber, agent, transaction.

Operator core systems remain in place.

Global public services without giving up sovereign control.

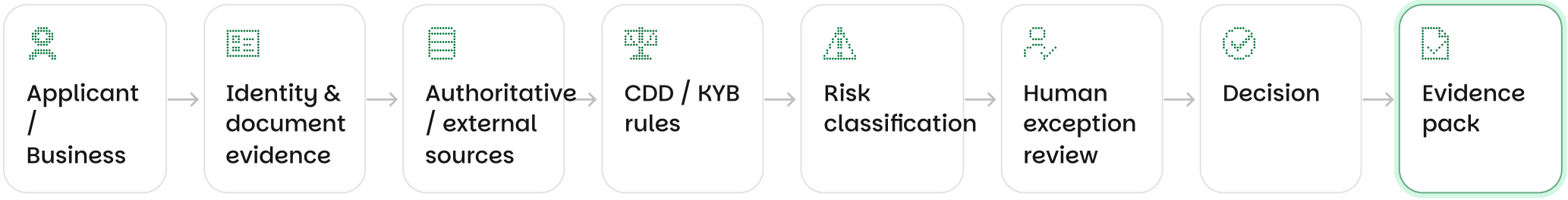


Seamfix trust infrastructure — underneath the process

ePass example. Application, identity proofing, approval, payment, renewal, delivery and status tracking go digital while the issuing authority keeps policy and decision control.

KYC/CDD evidence, not just onboarding.

The difficult part is rarely the form. It is the sequence of evidence, policy, source calls, manual exceptions and decisions behind the form.



Reduce avoidable friction

Increase decision defensibility

Commercial models that fit the programme.

Assess

Focused, fixed scope

One-off

You may stop here. The recommendation is yours to use with any supplier.

Implement

Fixed, milestone, outcome-based or T&M

One-off or milestone

Platform licence

Agreed production scope

Recurring

Operate

Managed operations

Optional, recurring

Programme-variable services — third-party verification, messaging or cloud — are disclosed in the proposal and contract rather than hidden inside the licence.

STANDARD ROUTES

- Conventional procurement
- Platform licence
- Managed service

STRUCTURED PROGRAMME MODELS · QUALIFYING PROGRAMMES

- PPP
- Vendor-financed
- Transaction-linked

Subject to legal, regulatory, credit and commercial approval.

Security, privacy and procurement assurance.

01 Legal entity & contracting

02 ISO management systems

03 Secure engineering

04 Privacy / data protection

05 Hosting / residency

06 Platform release lifecycle

07 Service operations / BCDR

08 Responsible disclosure

- ISO/IEC 27001 — information security
- ISO/IEC 27701 — privacy information
- ISO 9001 — quality management

Hosting and residency are agreed per programme. Current certificates, scope and the security & procurement pack are available through the Trust Centre.

Tell us what has to work.

Bring us one process that is slow, exposed, hard to verify or difficult to defend. We will help define the smallest useful first step.

seamfix.com/contact

United States · United Kingdom · United Arab Emirates · Africa

Trusted Digital Identity for Every Human