

A SOVENTRA SOLUTION

SHAHIN AI



Governance, security operations and governed intelligence.

A practical guide to the platform, its delivery scope and the outcomes BrightGate helps your team put into operation.

GRC

Requirements to evidence

SOC

Signal to response

AI

Human oversight

BrightGate product and professional-services overview. Prepared 26 September 2026. Product availability, editions and implementation scope are confirmed in your proposal.

01 / GOVERN

A record your team can explain.

SHAHIN GRC connects obligations, controls, owners and evidence so that assessments can lead to accountable follow-up.

01

Define
requirements

02

Assign controls

03

Assess & evidence

04

Track remediation

Governance & risk

Organise policies, accountability, risk assessment and treatment decisions. Give each action an owner and a review path.

Compliance & evidence

Assess requirements, link supporting records and follow remediation. Reuse controls while preserving the source of each obligation.

Audit & oversight

Coordinate requests, findings and management responses. Use reporting to show progress, outstanding gaps and decisions.

Privacy & third parties

Bring privacy obligations and supplier exposure into scoped assessment workflows with defined access and responsibilities.

A practical engagement

BrightGate can help establish the scope, map the initial controls, organise evidence, configure workflows and train the control owners. Your handover can include a configured register, evidence structure, gap report and prioritised action plan.

02 / DEFEND

From a security signal to an informed response.

SHAHIN SOC supports monitoring, detection, triage, investigation and coordinated response within the agreed operating model.

01

Collect telemetry

02

Review alerts

03

Investigate cases

04

Approve response

Monitoring & detection

Connect agreed event sources and detection logic. Review alert context and prioritise the next investigation step.

Cases & investigation

Bring related signals, timelines, analyst work and evidence together so findings can be reviewed and followed through.

Threat context

Use threat intelligence, hunting and security analytics to inform investigations and refine detection use cases.

Controlled response

Prepare and verify actions through defined permissions, policies and human approval. Integration scope is agreed per project.

BrightGate delivery outputs

A scoped source-onboarding plan; configured integrations and detection use cases; documented alert-to-case tests; access roles; operating runbooks; and analyst handover. Platform deployment is separate from any contracted 24/7 monitoring service.

03 / DECIDE

Useful intelligence. Defined authority.

Optional AI assistance supports analysis and proposed work within authorised knowledge, tools and approval boundaries.

01

Set objective

02

Prepare a proposal

03

Human review

04

Verify & record

Governed agent work

The published operating model coordinates specialists, reviews proposed actions, applies human and policy control, and preserves execution evidence. Confirm enabled capabilities in the selected release.

Knowledge & permissions

Relevant enterprise knowledge can ground assistance. Domain-scoped roles and defined tool permissions keep work aligned to organisational responsibilities.

Deployment choices

Self-hosted and private environments are described by the vendor. Identity integration, isolation and data residency depend on infrastructure and configuration.

A connected platform

Reusable libraries, versioned evidence, recurring tasks and configurable dashboards support daily GRC operations. Logical domain scoping is distinct from isolated tenancy.

During discovery, BrightGate confirms the data boundary, identity model, enabled AI functions, integration prerequisites and acceptance measures. No unsupported automation or regulatory certification is implied.

Product source: Governed AI

Product source: Platform & access model

04 / DELIVER

From discovery to a working capability.

BrightGate provides exclusive KSA distribution and professional services for SHAHIN AI, as part of the partnership stated by BrightGate.

01 Discover & scope

Confirm entities, users, applicable obligations, priority workflows and success criteria. Output: an agreed scope and implementation plan.

02 Configure & integrate

Set up the agreed environment, access model, content, workflows and supported connectors. Output: a configured solution with documented design decisions.

03 Validate & enable

Run agreed scenarios, record findings, resolve implementation gaps and train administrators and business owners. Output: acceptance evidence and operating guidance.

04 Handover & plan forward

Transfer the configuration, knowledge and open-item register. Output: an accountable handover and a scoped next-phase roadmap.

Book a focused demonstration.

info@brightgate.com.sa | +966 54 546 4009

The platform supports compliance work; it does not guarantee compliance or certification. Libraries and regulatory applicability require scope and version review. Services, support hours and integrations are defined in the commercial proposal.