SECURITY GOVERNANCE

OmniGuard

Connect assets, risks and security controls in one governance workspace

Give security and risk teams a shared view of assets, control ownership, exposure and improvement work.

The value for your team

01

Shared context

Connect assets, obligations, controls and evidence in one workspace.

02

Visible ownership

Make control and remediation responsibility easier to follow.

03

Better priorities

Focus improvement work using risk and operating context.

Product overview

OmniGuard brings operational security governance into one coherent view. It helps teams organise what must be protected, which controls apply, where evidence sits and who owns the next action—without pretending that a dashboard replaces the underlying security tools or expert judgement.

OmniGuard is designed for security, risk and compliance teams that need a common operating picture across controls and remediation. It connects asset and service inventory, evidence registers and review and audit support so teams can move from input to accountable action without losing the decision trail.

The product supports the operating workflow; it does not remove professional judgement, statutory responsibility or customer ownership. Final controls, integrations and commercial scope are confirmed during discovery and recorded in the implementation plan.

Customer challenges it addresses

01 Information about asset and service inventory, risk and control mapping and evidence registers often lives in separate tools, inboxes or spreadsheets, making the operating picture difficult to trust.

02 When teams need to link controls, evidence and gaps, manual hand-offs can hide ownership, delay decisions and make exceptions harder to resolve.

03 Leaders need a clearer way to achieve better priorities while preserving human approval, role boundaries and an understandable record of what happened.

Value created in practice

Shared context

Connect assets, obligations, controls and evidence in one workspace.

Visible ownership

Make control and remediation responsibility easier to follow.

Better priorities

Focus improvement work using risk and operating context.

Detailed capabilities

Six connected capabilities shape the core OmniGuard operating experience.

01 Asset and service inventory

Maintain a governed view of the assets and services that require protection and control ownership.

02 Risk and control mapping

Connect relevant risks and obligations to the controls intended to address them.

03 Evidence registers

Organise supporting material around the relevant matter or review so users can understand provenance and purpose.

04 Remediation ownership

Assign corrective work, follow status and preserve closure evidence without losing the original finding context.

05 Governance dashboards

Summarise control coverage, ownership and improvement work for governance review.

06 Review and audit support

Keep service interactions connected to the customer record so commercial and delivery teams share the same context.

Connected operating model

The capabilities are designed to work together. Asset and service inventory establishes context, evidence registers moves the work forward, and review and audit support supports review and accountability.

How teams use the product

The workflow is intentionally simple to understand, while retaining visible owners, review points and evidence.

01

Map critical assets and obligations

Authorised users combine asset and service inventory and risk and control mapping to map critical assets and obligations. The workflow keeps the responsible owner, review point and resulting action visible.

02

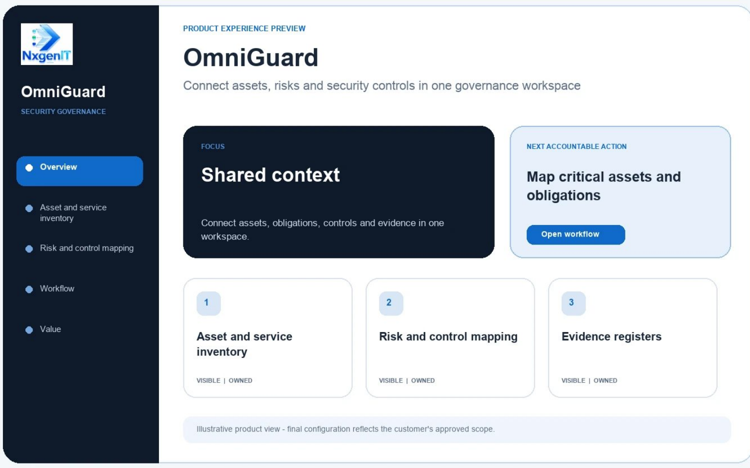
Link controls, evidence and gaps

Authorised users combine evidence registers and remediation ownership to link controls, evidence and gaps. The workflow keeps the responsible owner, review point and resulting action visible.

03

Prioritise and govern improvement work

Authorised users combine governance dashboards and review and audit support to prioritise and govern improvement work. The workflow keeps the responsible owner, review point and resulting action visible.



Illustrative product preview. Final screens and configuration reflect the customer's approved scope.

Rollout, governance and success

A controlled rollout keeps the product aligned to customer ownership, real operating roles and measurable outcomes.

PHASE 01

Discover and scope

Confirm the users, operating boundaries, source data and decisions that OmniGuard must support.

PHASE 02

Configure roles and controls

Define authorised roles, approval points, protected information and escalation paths before customer data is introduced.

PHASE 03

Prepare data and connections

Map the required inputs for asset and service inventory and risk and control mapping, including migration or integration needs.

PHASE 04

Pilot, validate and scale

Run a controlled pilot, review outcomes with responsible users, adjust the workflow and expand only after acceptance.

Roles, ownership and control

OmniGuard is configured around named users, authorised roles and explicit approval points. Customer data remains customer-owned, protected information is limited to appropriate roles, and important actions retain an understandable history.

What success can look like

- Shorter cycle time across 'Map critical assets and obligations'.
- Fewer unresolved exceptions around evidence registers.
- Clearer ownership of approvals, follow-ups and closure evidence.
- Stronger adoption among the intended users and responsible reviewers.

Best for

Security, risk and compliance teams that need a common operating picture across controls and remediation.

See how this product fits your operation

www.nxgenit.co.za/products/omniguard | info@nxgenit.co.za