

SIG Lite Responses

Standardized Information Gathering (Lite) — pre-filled responses

Reflects Global Barry's current security posture as of **October 2, 2026**. Items not yet in place are marked **In progress**; nothing in this document asserts a certification Global Barry does not hold.

A streamlined, SIG Lite-style questionnaire completed by Global Barry covering operational risk, data storage protocols, access control, encryption and business continuity. Authored by Global Barry; it is not an official Shared Assessments deliverable.

A. Enterprise & Operational Risk

ID	Question	Status	Global Barry response
A.1	Describe the service.	Yes	Public-source-first financial intelligence platform: company intelligence, exposure analysis, research copilot, watchlists/portfolios, alerts and a read-only API. No trading, custody or market-data resale.
A.2	Independent assurance report available?	In progress	Global Barry runs on enterprise cloud infrastructure (AWS / Google Cloud / Abacus.AI). The providers' data centers maintain SOC 2 Type II and ISO 27001 attestations, published by those providers. Global Barry does not currently hold its own SOC 2 Type II report or ISO 27001 certificate; pursuing its own SOC 2 Type II via automated compliance tooling (e.g. Vanta or Drata) is In progress .
A.3	Is there a risk assessment programme?	In progress	Formal periodic risk assessment is being established under the SOC 2 programme.

B. Data Storage Protocols

ID	Question	Status	Global Barry response
B.1	Where and how is customer data stored?	Yes	Managed hosted PostgreSQL; records are scoped per account (account-owned session identifiers).
B.2	How are API credentials stored?	Yes	Global Barry API credentials (bkg_<prefix>_<secret>) are stored only as a one-way SHA-256 hash plus a short public prefix. The secret is shown once at creation/rotation and cannot be recovered or reversed.
B.3		Yes	

	How is customer financial data used?		Portfolios, watchlists and holdings are stored per account in Global Barry's account database, sent to Global Barry's managed AI inference endpoint only transiently when the user asks an AI question, never sold, never shared with third parties, and never used to train global/foundation models.
B.4	Is customer data used for model training or shared?	No	Never used to train global/foundation models; never sold; never shared with third parties.
B.5	Are third-party keys collected from customers?	No	No. AI runs on Global Barry's managed inference endpoint.

C. Access Control

ID	Question	Status	Global Barry response
C.1	User authentication	Yes	Email + password (salted one-way hash); opaque, server-side-hashed session tokens; CSRF double-submit protection.
C.2	API access	Yes	Read-only scoped credentials, per-key rate limit, plan entitlements, rotation and revocation.
C.3	Privileged access	Yes	Admin surfaces gated by a separate shared secret; not in public navigation.
C.4	SSO / MFA	In progress	On the roadmap.

D. Encryption

ID	Question	Status	Global Barry response
D.1	Encryption in transit	Yes	HTTPS for all public endpoints; TLS terminates at the platform edge.
D.2	Encryption / protection at rest	Partial	Credentials are one-way hashed; storage-level encryption is provided by the managed infrastructure provider.
D.3	Customer-held keys	Partial	Bring Your Own Vault (AWS Secrets Manager, Azure Key Vault, HashiCorp Vault) via request-time injection — enterprise option on request.

E. Business Continuity & Backup

ID	Question	Status	Global Barry response
----	----------	--------	-----------------------

E.1	Service resilience	Yes	Supervised processes with automatic restart; health endpoint; version-controlled deployment configuration with restore points.
E.2	Backups	Partial	Database hosted on managed PostgreSQL infrastructure; formal backup-restore testing with defined RPO/RTO is In progress.
E.3	Documented BC/DR plan	In progress	Being documented as part of the SOC 2 programme.

F. Incident Management

ID	Question	Status	Global Barry response
F.1	Security contact	Yes	security@barryglobal.com
F.2	Incident response plan	In progress	Formal plan with notification timelines being documented; credentials can be revoked immediately.