

CAIQ Responses

Consensus Assessments Initiative Questionnaire — CAIQ-aligned 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.

Global Barry's own responses, organised by the control domains of the Cloud Security Alliance's Consensus Assessments Initiative Questionnaire (CAIQ). This is a **CAIQ-aligned** summary authored by Global Barry; it does not reproduce CSA question text and is not a CSA STAR registration.

Attestation status: 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**.

Application & Interface Security

ID	Question	Status	Global Barry response
AIS-01	Are applications designed and developed according to secure coding practices?	Yes	Server-side input validation (e.g. strict CIK/identifier validation), output escaping in templates, and automated test suites covering API security behaviours (dotfile blocking, auth and cache headers).
AIS-02	Are customer-facing APIs authenticated and rate limited?	Yes	Public API requires a Global Barry API credential; per-key rate limits (default 60/min) and plan quotas are enforced. Global Barry API credentials (<code>bgk_<prefix>_<secret></code>) 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.
AIS-03	Is web session state protected against CSRF and hijacking?	Yes	Opaque session tokens stored server-side as hashes; HttpOnly, SameSite=Lax cookies; double-submit CSRF protection on state-changing requests.

Audit Assurance & Compliance

ID	Question	Status	Global Barry response
AAC-01	Does the organisation hold an	In progress	Global Barry runs on enterprise cloud infrastructure (AWS / Google Cloud / Abacus.AI). The providers' data centers

	independent audit report (e.g. SOC 2 Type II)?		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 .
AAC-02	Can infrastructure provider attestations be provided?	Yes	Provider SOC 2 / ISO 27001 reports are published by AWS and Google Cloud through their own compliance portals; Global Barry can point reviewers to them. These attest to the provider, not to Global Barry.

Business Continuity & Operational Resilience

ID	Question	Status	Global Barry response
BCR-01	Are services monitored and automatically restarted on failure?	Yes	Application processes run under systemd supervision with automatic restart; a health endpoint is available.
BCR-02	Is there a documented, tested business continuity / DR plan?	In progress	Database runs on managed hosted PostgreSQL; a formal, tested BC/DR plan with defined RTO/RPO is being documented as part of the SOC 2 programme.

Change Control & Configuration Management

ID	Question	Status	Global Barry response
CCC-01	Are changes version controlled and tested before release?	Yes	All code and deployment configuration (service units, web server vhosts) are version controlled in git with restore points; automated tests run before release.
CCC-02	Is there a formal change-approval workflow with segregation of duties?	In progress	Formal change-approval and segregation-of-duties controls are planned with the SOC 2 programme.

Data Security & Information Lifecycle

ID	Question	Status	Global Barry response
DSI-01	How is customer financial data stored and segregated?	Yes	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.
DSI-02	Is customer data used to train AI models or	No	No. Customer financial data is never used to train global/foundation models, never sold and never shared with third parties.

	shared with third parties?		
DSI-03	Does the product require customers to supply third-party API keys?	No	No. AI features run on Global Barry's own managed inference endpoint; there is no place in the product where customers enter third-party keys.

Encryption & Key Management

ID	Question	Status	Global Barry response
EKM-01	Is data encrypted in transit?	Yes	Public endpoints are served over HTTPS; TLS terminates at the platform edge before traffic reaches the application host.
EKM-02	How are API credentials protected at rest?	Yes	Global Barry API credentials (bgk_<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.
EKM-03	Can customers keep custody of their own keys (BYOK / vault)?	Partial	Bring Your Own Vault (AWS Secrets Manager, Azure Key Vault, HashiCorp Vault) with request-time credential injection is offered as an enterprise deployment option arranged on request; it is not a self-serve integration.

Governance & Risk Management

ID	Question	Status	Global Barry response
GRM-01	Are security policies documented and published?	Partial	Security posture is published in the public Trust Center. A formal information security policy set is being completed under the SOC 2 programme (In progress).
GRM-02	Is AI output governed to prevent fabricated claims?	Yes	AI responses are tiered FACT / INFERENCE / ANALYSIS / UNKNOWN, citations are validated against ingested public records, and guards prevent price-causation and investment-advice statements.

Identity & Access Management

ID	Question	Status	Global Barry response
IAM-01	Are user passwords stored securely?	Yes	Passwords are hashed with a salted, one-way algorithm (Werkzeug security helpers); plaintext passwords are not stored.
IAM-02	Is administrative access restricted?	Yes	Administrative surfaces are gated by a separate shared secret and are not linked from public navigation.

IAM-03	Is SSO / SAML and MFA supported?	In progress	Enterprise SSO and MFA are on the roadmap.
--------	----------------------------------	-------------	--

Infrastructure & Virtualization Security

ID	Question	Status	Global Barry response
IVS-01	Where is the service hosted?	Yes	Enterprise cloud infrastructure (AWS / Google Cloud / Abacus.AI) with managed PostgreSQL. Physical and environmental controls are inherited from the provider.
IVS-02	Is the network perimeter restricted?	Yes	Only HTTPS ingress and administrative SSH are exposed; the web server blocks dotfiles, deployment files and source files and sets security headers.

Security Incident Management

ID	Question	Status	Global Barry response
SEF-01	Is there a security contact for reporting incidents?	Yes	security@barryglobal.com
SEF-02	Is there a documented incident response plan with notification timelines?	In progress	A formal incident response plan with customer notification timelines is being documented under the SOC 2 programme. Compromised API credentials can be revoked immediately.

Supply Chain Management, Transparency & Accountability

ID	Question	Status	Global Barry response
STA-01	Which subprocessors handle customer data?	Yes	Cloud infrastructure and managed database providers, and the managed AI inference endpoint (Abacus.AI infrastructure) used transiently for inference. No data is sold or shared with other third parties.
STA-02	What data sources power the intelligence?	Yes	Public-source filings and disclosures (e.g. SEC, BEA, BLS, Federal Reserve, Treasury) with provenance retained; no commercial market-data feeds.