GABI FAQs - Information Security

1. What are GABI-PRIME and GABI-GEO?

GABI-PRIME and GABI-GEO make up our proprietary, online Gap Analysis & Benchmarking Insights tools, developed by the Risk Coalition Research Company Limited in association with Independent Audit Limited. They aim to help clients better understand and efficiently implement either:

- the Risk Coalition's 'Raising the Bar – principles-based guidance for board risk committees and risk functions in the UK financial services sector'.
- Or the Risk Coalition's 'The Extra G – ESG^2 - Principles-based guidance for Geopolitical risk oversight and its integration with ESG issues for boards, risk committees and risk functions'.

Access to GABI-PRIME or GABI-GEO is provided on a subscription basis and no software is installed in the client environment.

2. What kind of information do our GABI tools capture?

Our GABI tools have been designed to capture board director and senior management views (anonymously) on how well the organisation meets the Raising the Bar or The Extra G - ESG^2 guidance and provides a comparative benchmark against peer organisations. As such, this information is sensitive but not business critical and does not involve transactions, customer information or financial data.

3. What personal data is processed?

Survey respondent name, email address, profiling fields, IP address, comments that might be used to identify an individual.

4. Is the Risk Coalition Research Company a data controller?

Yes, for the limited personal information we maintain.

5. Browser support

GABI tools are accessed using a web browser. The following browsers are supported:

- IE8+ and Edge for Windows
- Firefox 35.0+ for Windows and Mac OS X
- Safari 7.1+ for Mac OS X and iOS
- Chrome 41.0+ for Windows

6. Who has access to GABI tools?

Local administrator access is normally provided to your Company Secretary (or other nominated administrator) for them to set up your own GABI users (questionnaire respondents).

Users are responsible for creating and using sufficiently secure passwords – but minimum standards are also built into GABI. Password parameters (length, complexity, etc) are set out below.

A small number of Risk Coalition Research Company administrators and those working for our service providers, Independent Audit Limited, have full access to the Production Environment, including client information (i.e. the collated responses to questions from Respondents). This is necessary for the initial client set-up and smooth operation of the service.

7. Are all communications encrypted?

Yes – GABI tools use AES 256 encryption for the database and uses TLS (256-bit encryption) when being accessed via the browser, over HTTPS. Data held in backup is also encrypted (using AES 256-bit encryption).

8. How is Risk Coalition Research Company and Independent Audit administrator access to GABI managed?

Risk Coalition Research Company administrator access is limited to two company directors. Independent Audit administrator access is limited to three employees. Each administrator has their own unique GABI user ID and password. Policy-based administrator password parameters are:

- Minimum of ten characters
- Minimum complexity of at least one upper and lower case character and a number
- No use of common or obvious passwords (e.g. names, words, etc)

9. How our information is kept separate from other clients' information?

When a client subscribes to any of our GABI tools, we set up a logically separate company entity in the GABI database. Client administrators and users only have access to their own client entity and cannot access any other company.

GABI is security-tested (penetration test) by an independent third party annually to ensure the application is robustly developed and appropriately secure.

10. What security protocols and ciphers are supported?

GABI supports the following protocols and ciphers:

Supported protocols:

- TLS 1.1
- TLS 1.2

Supported ciphers:

- Triple DES 168
- AES 128/128
- AES 256/256
- SSL – all versions
- PCT 1.0

11. Where is our information stored?

GABI uses a virtual server hosted by Amazon Web Services. The Amazon datacentre is based in Ireland and conforms to industry best practice standards. Go to http://aws.amazon.com/ec2/ for more information.

12. How is our information secured?

Clients access the GABI web portal using 256-bit TLS encryption to create a secure pipe between the user's machine and the GABI web server. The server is protected by Amazon Security Groups. All data storage, processing, analysis and reporting is performed using applications installed on the virtual GABI server and does not leave the box other than for report preparation and printing by the client administrator.

Client data is segregated through creation of a virtual private database for each client that encrypts data at rest and logically separates it from any other client's data.

13. What happens to our information if we cancel our subscription?

Anonymised client data will be retained for the purposes of benchmarking. Client personal information will be securely deleted upon confirmation that a subscription will not be renewed.

14. How is logical access to the GABI server secured?

Logical access to the GABI server is protected by Amazon Security Groups, maintained and managed by Independent Audit and their contracted software developer, Logrus. Connections are restricted to HTTPS.

15. What server maintenance and resilience arrangements do you have in place?

As part of Independent Audit's contract with Logrus, the latest Microsoft Windows Server 2016 patches are applied to the to the GABI virtual server on a monthly basis using a defined maintenance protocol. Logrus tests all patches in separate testing environment before installing them.

Data is backed up through an incremental hourly snapshot and an incremental daily and full weekly back up of all GABI data. Backed up data is held securely in a separate part of the Amazon S3 Storage (http://aws.amazon.com/s3/) in Amazon's Frankfurt centre. Since we use a virtual GABI server, there is no risk of hardware failure and all data can be restored quickly and safely on an instantly created new virtual server.

16. What third parties have access to GABI (other than clients)?

Currently, third parties are limited to Independent Audit Ltd, and their contracted developers Logrus (UK) LLP. Logrus is incorporated and based in the UK but has offshore development resources based in Eastern Europe. Logrus provides Independent Audit with dedicated MCSD (Microsoft Certified Solutions Developer) qualified resources and applies standard software development best practices. No Logrus employees or contractors are permitted access to the Production database. GDPR compliant model clauses relating to the transfer of personal data to processors based in countries outside of the EEA are in place between the Risk Coalition Research Company, Independent Audit and Logrus to ensure the appropriate protection of personal data.

In case of emergency “break glass support”, and subject to client approval, Logrus may be granted access to the server but new passwords are put in place immediately once a solution has been implemented.

Contact

For GABI-PRIME please contact Chris Burt: +44 (0)20 3823 6569

chris.burt@riskcoalition.org.uk

For GABI-GEO please contact: Derek Leatherdale: +44 (0) 20 7459 4779

derek.leatherdale@riskcoalition.org.uk