EiQ FAQs

Version 2.0

Contents

1 General information

1.1 What is EiQ and how does it work?

EiQ is LRQA's supply chain due diligence assurance platform. The platform is divided into three sets of modules: risk exposure, analytics, and risk management.

- Risk exposure uses EiQ's proprietary data sets built on audit records, trusted civil society datasets, and adverse media to undertake due diligence on the most salient forms of supply chain ESG risk across a production region, product or service category, or entity based on our assessment of inherent risk.
- Analytics uses our datasets on inherent risk and managed risk – risk specific to a site, derived from your audit data – to provide a wholistic understanding of the risk profile of your suppliers. Analytics also allows users to create risk maps that are specific to your supply chain's operations, segmenting your supplier base by a suggested risk treatment.
- Risk management digitalizes your audit records, enabling a systematic approach to program benchmarking and reporting, using industry comparable to inform an assessment of your supply chain's performance.

1.2 What type of risks does EiQ assess?

Our ratings cover five ESG pillars: issues associated with labor, health and safety, environment, business ethics, and management systems. Scores are produced for each pillar, supported by 50+ sub-indices covering issues ranging from forced labor and child labor to building safety, wastewater management, and wage documentation. For more detail on the forms of risks we cover, please see our methodology document.

1.3 How does EiQ gather and analyze data?

LRQA audit data is derived from the 25,000+ onsite audits we conduct annually as well as third-party audit data – irrespective of your audit standard. Data sources integrated into EiQ also include trusted civil society datasets such as the United Nations and International Labor Organization (ILO). EiQ also includes data gathered through our adverse media screening tool, Sentinel, which scans for instances of ESG risk across 250,000+ entities each month.

1.4 Can EiQ be customized for our specific supply chain needs?

What separates EiQ is its ability to tailor data to the needs of your supply chain or responsible sourcing program, enabling you to answer the most pressing concerns that your program faces: be they related to compliance with emerging supply chain due diligence laws or your program's effectiveness.

1.5 Is EiQ compatible with existing supply chain management systems?

Yes! EiQ is a fantastic supplement to your current supply chain management systems. It streamlines and enhances data integration, risk management, supplier onboarding, risk monitoring, program benchmarking, internal and external reporting, supplier engagement, and stakeholder transparency. The platform improves upon any current procurement management system.

1.6 Are you able to integrate non-LRQA audit data into your assessment of a company's supply chains?

Yes, ownership rights permitting, we are able to build in non-LRQA audit data into your account.

1.7 What level of technical expertise is required to use EiQ?

EiQ is accessible for any position or expertise level. Most of our users do not have any background in data analytics. We provide comprehensive user guides and how-to instructions to assist with any useability questions. A dedicated Customer Success Manager is also assigned to each account, supporting the onboarding of individuals – irrespective of their position in the organization.

2 Risk exposure (Geography & product risk ratings, Sentinel)

2.1 What is the risk exposure module in EiQ?

EiQ's risk exposure module contains inherent ESG risk data for countries, regions, products and service categories. The risk exposure module contains four sections: global risk landscape, geography risk landscape, product risk landscape, and Sentinel.

2.2 What is a supply chain ESG risk rating?

A supply chain ESG risk rating provides an overview of where ESG risk violations are most likely to occur within your supply chain. A region, product, service, or site is scored on a 10-point gradient. Sites that are rated closer to zero are judged as having extreme exposure to supply chain ESG risk. Extreme risk suggests a greater likelihood of supply chain ESG violations occurring within. A region, for a product or service category, or site.

All scores are on a 0-10 scale:
O-2.49 = Extreme risk: Very high frequency of violations. Needs regular intervention. (**Red**)
2.5- 4.99 = High risk: Frequent instances of violations identified. Needs intervention. (**Orange**)
5- 7.49 = Medium risk: Moderate frequency of violations. Needs guidance. (**Yellow**)
7.5- 10 = Low risk: Limited to no instances of violations. Needs monitoring. (**Green**)

2.3 What sources contribute to the risk ratings?

Geography and product risk ratings are derived from three sources:

- Social and environmental audit data: LRQA conducts more than 25,000 social and environmental assessments per year across the global supply chain. Assessment data are standardized and aggregated at country, sector and province/state level – irrespective of the standard. We most commonly work with ERSA, LRQA's Responsible Sourcing Audit tool. We also support integration of third-party data sets from other providers, including SLCP, ICS, RBA, SMETA, and BSCI.
- Civil society datasets: LRQA leverages public domain data from multilateral organizations and NGOs to complement risk information where audits are less likely to evidence specific violations – e.g., forced labor – or in low sample countries. Not every dataset available is considered in EiQ. Some datasets covered include those provided by the World Bank, the World Justice Project, the UN, and UNICEF.
- EiQ Sentinel Data: EiQ uses adverse media from local news sources in sourcing countries, external compliance datasets, specialized press, and search engines to regularly scan for risk events. Coverage spans risk events reported in 100+ local languages.

2.4 How frequently are the risk ratings updated?

Our ratings are updated bi-annually.

2.5 How many countries and regions are covered in the ratings?

Our ratings are available for 100+ countries/provinces, dependent on where data is available. Countries with provincial data include China, United States, India and Vietnam.

2.6 How many years of data are calculated into the risk ratings?

Our datasets date back to 2016.

2.7 What do confidence levels indicate?

Confidence scores are based on the volume of audit data conducted in the area. Areas with lower confidence scores integrate civil society datasets to provide a more comprehensive rating. Each country or province has a confidence score indicated below its rating.

2.8 What is Sentinel and how does it contribute to risk exposure?

Sentinel is EiQ's adverse media-scanning tool. Sentinel scans thousands of media channels for ESG incidents (positive or negative) related to EiQ's supplier database of more than 150,000 suppliers. Sentinel contributes to risk exposure through:

- Integration into geography risk ratings, which supplement the limitation of traditional due diligence data. Sentinel's capability in identifying issues such as fire incidents, harassment and abuse, forced labor and freedom of association non-compliances in close to real-time significantly strengthens the robustness of our geography risk ratings.
- Integration into the calculation of product level risk ratings.

2.9 What is the process by which Sentinel results are reported?

1. Formulate searches: The client provides our data team with the name and address of the site they would like scanned and our team reviews and reconciles the information with our LRQA database.
2. Source data: Based on this data input, Sentinel then conducts a web scan and scrape on the 14th of each month of more than 250,000 entities. The Sentinel algorithm then extracts the entity name and matches the incidents to ensure they are relevant to the keywords identified and a manual search is done by our data team to identify the incidents related to the site and keywords.
3. Find and clean relevant data: The data is then cleaned and manually checked by our data team to minimize false positives.
4. Release findings: Sentinel hits are organized, summarized, and released on the EiQ platform around the 10th of each month.

2.10 How often are Sentinel scans conducted?

Sentinel scans are conducted monthly. EiQ users may request to add suppliers to new scans if there is not readily available data on them. The cutoff to add new suppliers to the scan is the 24th of each month. Results will become available on EiQ after 10 business days, after a round of review by an analyst.

2.11 How do I see results in Sentinel that are specific to my supply chain?

Select the "My Program" under filters to view results only from factories linked with your program.

3 Risk management (Program trend reports, supply chain benchmarking)

3.1 How does the risk management module support in responsible sourcing decision-making?

The risk management module harnesses data and analytics to promote supply chain ESG risk monitoring and mitigation. This module offers insights that guide strategic actions and enhance the overall sustainability and ethical performance of the supply chain. It improves decision-making by helping executives:

- Identify suppliers that may be facing ESG-related challenges and take proactive measures to address these issues.
- Allocate resources more effectively as it categorizes risk based on severity, allowing executives to prioritize efforts based on the most critical issues
- Benchmark against wider industry data, which can inform sourcing strategies, supplier negotiations, and program enhancements.
- Enable proactive risk mitigation through real-time visibility into ESG risks across the supply chain.

3.2 How frequently are program trend reports generated?

Program trend reports are reported in real-time. After an audit report is complete, your data will be integrated into program trend reports no later than 10 working days from when the report was issued.

3.3 What is supply chain benchmarking?

Supply chain benchmarking is a process in which a company compares its supply chain performance, practices, and metrics against those of other companies or industry best practices. The goal of supply chain benchmarking is to identify areas for improvement, optimize processes, and drive performance enhancements within the supply chain.

3.4 How is my benchmark chosen?

Audit programs require any site to list the sector for which an audit is undertaken. This sector level designation then informs how your data will be reported in EiQ.

3.5 Can I customize the parameters for supply chain benchmarking?

Absolutely, the benchmarking features in program trend reports are completely customizable based on various ESG metrics and timelines.

3.6 Can I request a demo or trial of EiQ?

Absolutely! You may request a demo through this link or by reaching out to one of your LRQA representatives and we will be happy to walk you through the platform.

4 Onboarding

4.1 What is the onboarding process like for new users of EiQ?

Onboarding is undertaken over a two-month time period. In this period of time, users will have their access to EiQ enabled, an initial series of onboarding meetings with their customer success manager, and will undergo a technical enablement process, which will integrate your supply chain data into the platform.

4.2 Can I request a personalized onboarding session for my team if we have already undergone the onboarding process?

Absolutely. Your customer success manager would be happy to schedule as many onboarding sessions as required to set up new users for your account on the platform.

4.3 How do I set up my initial EiQ account?

Your customer success manager will activate your account upon onboarding. One or more account administrators will be assigned to your account. Other team members wishing to use EiQ must request an invitation to join your account. If you don't know who your account administrator is, email support@eiqsupport.freshdesk.com to identify the account. Please do note that sharing login information violates LRQA's terms and conditions.

4.4 Is customer support available for EiQ?

EiQ customer support is currently available across most time zones. We have customer support representatives in the US, Europe, and Hong Kong to assist with any questions or concerns. Should you require customer support but be unsure of who your appointed customer success manager is, please reach out to support@eiqsupport.freshdesk.com.

4.5 What is the average response time for customer service inquiries?

One of our customer service reps will get back to you within 24 hours of your inquiry.

4.6 I would like to segregate access to my supply chain data across my EiQ account. How?

Your customer success manager will be able to create separate accounts for each part of your organization should you wish to limit the visibility that certain parts of your organization have to the operations of another part of your organization. Please contact your customer success manager for setup.

5 Customer service

5.1 How do I provide feedback about my customer service experience?

We love hearing feedback – and while we hope that you do not have any problems with our customer service team, please do not hesitate to reach out should you find your service dissatisfactory. All feedback can be submitted here.

6 Updates & roadmap

6.1 How often do you release updates? What's on the product roadmap?

Product updates are typically released every two months. Users will be updated on EiQ's developments through a regular touch base with your dedicated customer success manager as well as through an email alert. CSMs would be happy to also speak to the broader development priorities of the platform.

7 Testimonials & case studies

7.1 Who are some of your notable clients?

Our clients include many of the world's largest consumer products, industrial goods, and service providers. Should you seek an understanding of common practices for any of these sectors, please do not hesitate to schedule a call with your customer success representative.

7.2 Do clients use EiQ for public reporting?

A number of clients use EiQ to support their public reporting requirements. These include Woolworths, Archer Daniels Midland, SunRice, Kathmandu, Puma, Fenix Outdoor, or Neiman Marcus.

8 Commercial

8.1 How do I upgrade or downgrade my EiQ subscription?

Access to EiQ is not modularized. Why? Because we believe that a full arsenal of ESG due diligence tools is needed to effectively manage any organization's exposure to supply chain ESG risk. The one exception that we may make for this though is for Sentinel, our adverse media scanning tool. We understand that you may need to undertake a one-off scan as a part of project-based due diligence. Should you wish to explore this, please do not hesitate to reach out to our sales team.

8.2 What is the refund policy for EiQ?

Great supply chain ESG due diligence requires a tremendous amount of effort: both on your organization and ours. No refunds are offered.

8.3 Are there any additional costs or fees associated with specific features or services?

There are none. We – as LRQA – do offer a large number of other business assurance products. Should you wish to inquire about these products, please do reach out to our sales team.

8.4 How do I cancel my subscription?

EiQ operates using an evergreen renewal structure. All those that seek to discontinue their subscription are requested to reach out to LRQA a year in advance of their renewal date.

8.5 Can I reactivate my account after cancellation?

Yes – you can. Do note that should you wish to reactive your account after a period of discontinued service, you will no longer be entitled to any historical pricing arrangement.

9 EiQ data security and privacy

9.1 How EiQ is architected?

The EiQ platform network security architecture consists of multiple security zones, development, staging, and production environments are separated from each other.

9.2 What is the user password policy?

Local database is used for user authentication, complex password is enforced (required all 4 sets: upper, lower, numeric, special character), password length is set to 16, while password history is configured to 24, password will be enforced to change on every 90 days.

9.3 What is EiQ's security compliance?

The EiQ platform is ISO27001 compliance, the ISO27001 certification can be shared upon requested.

9.4 How often is third party penetration test conducted?

Web application pen test is conducted at least annually as per the ISO27001 requirement. Pen Test reports can be shared upon request.

9.5 What is the network vulnerability scan process?

There is a weekly internal vulnerability scan configured in EiQ, as well as a daily external application scan. All security vulnerabilities identified as 'High' and above are fixed according to the below timeline.

Rating	CVSSv3	Internet facing target resolution day	Non-internet facing yarget resolution day
Critical	9.0 – 10	2 days	7 days
High	7.0 – 8.9	30 days	30 days
Medium	4.0 – 6.0	90 days	No time frames
Low	0.1 – 3.9	No time frames	No time frames

9.6 Is there a source code review?

All application codes will undergo a thorough review to ensure compliance with coding standards, best practices, and to enhance software quality and maintainability. Additionally, the review will assess the presence of vulnerable third-party/open-source libraries and identify potential vulnerabilities.

9.7 How are security vulnerabilities managed?

Security patches will be applied monthly, and ad hoc security patching (zero-day security vulnerability) will be applied ASAP when required.

9.8 Is DDoS mitigation service covered?

All web applications were configured and protected by AWS CloudFront; DDoS mitigation service is covered.

9.9 What service is used for intrusion detection and prevention?

AWS GuardDuty service is enabled to ensure service ingress and egress points are instrumented and monitored to detect anomalous behaviour.

9.10 What malware protection is used?

AWS GuardDuty Malware Protection is enabled to detect the potential presence of malware.

9.11 Are threat intelligence programme utilised?

Several well-known threat intelligence programmes (e.g., Cert.org, Microsoft etc.) are utilised to monitor threats posted and act based on risk.

9.12 How are web applications protected?

All web applications are protected by AWS Web Application Firewall. Network Access Control List and Security Group were configured to allow only legitimate inbound connections based on business needs.

9.13 How is EiQ access monitored?

Administrative access to EiQ Platform is restricted on an explicit need-to-know basis, utilises least privilege, is frequently audited and monitored, and is controlled by our Operations Team. VPN connection with multiple factors of authentication is required for authorised staff to access the platform.

9.14 Is security awareness training conducted?

Information Security Awareness and Data Protection (GDPR) training is mandatory. The training courses will be updated and enrolled for all staff annually.

9.15 Is developer training conducted?

Developer training on OWASP is an essential requirement, all developers will be automatically enrolled in the course annually to refresh their understanding and proficiency in secure software development practices.

9.16 Is our data encrypted?

EiQ data is encrypted by secure protocol - HTTPS TLSv1.2 is enforced when data in transit. Data at rest is encrypted with AES-256 encryption algorithm.

9.17 How is personal information handled?

All personal information will be anonymised and deidentified (with no possibility of re-identification) in any reports.

9.18 How long is data retained?

All data will be kept according to the guideline below, LRQA will not keep records longer than required.

Retention period	Details	Deadline of data destruction
Immediately	Documents that we no longer have a business need to keep.	N/A
7 months	Any information that has been classified, that cannot be deleted immediately but the need to retain does not extend beyond seven months.	Retention period + 7 months.
14 months	Data that needs to be compared with the previous year.	
4 years	Default retention period unless the information belongs in one of the other periods.	
5 years	All Social Compliance audit raw data (hard copies and electronic files) will be retained for Five (5) years post-assessment as per APSCA requirement.	
7 years	Information such as expired contracts which may be needed for litigation.	
Over 7 years	By exception only, any information where there is a regulatory/legal requirement, or a compelling business need to keep it beyond seven years.	

Forever	Accounting files created/generated/processed in related to the Businesses in China (e.g., Financial Statements and Reports, General Ledger Data, Accounts Payable and Receivable Data, Tax Records, Budgets and Financial Forecasts, Auditing and Compliance Records, Bank and Financial Statements, Insurance data, etc) Reference: https://www.64365.com/zs/1805136.aspx	N/A

9.19 How is data privacy and security ensured when using EiQ?

When using EiQ, data privacy and security are ensured through a multi-faceted approach. We are committed to processing received data solely for the purpose of fulfilling the scope of your contract. To bolster security, we employ various measures, including identity and access checks using an authentication system, encryption of passwords, and data protection by default. Access rights are strictly limited, and all critical system updates are promptly installed. The service uses the TLS/HTTPS protocol for secure data transmission and protects its services with firewalls. Furthermore, to safeguard against data loss, we perform regular backups and incorporate a range of technical and organizational measures to maintain data integrity and safety.

9.20 Where can I access LRQA's privacy policy?

LRQA's privacy policy is available online LRQA respects privacy and is committed to online data security for public access.

9.21 What are your terms of service?

Our standard terms & conditions can be accessed here https://www.lrqa.com/en/terms-of-use/

9.22 How do you handle data breaches?

When we become aware of a data breach, we take immediate steps to address and mitigate its impact. **We notify the controller of any personal data breach, ASAP, within 72 hours after discovering it**. We notify the controller of any personal data breach ASAP within 72 hours after discovering it. This notification includes a description of the nature of the breach, the number of affected data subjects and personal data records, potential consequences, and the measures we have taken or proposed to address the breach. If the breach poses a high risk to the rights and freedoms of natural persons, we also communicate the breach to the affected data subjects. Depending on our agreement with the client and the nature of the breach, we might also communicate the breach to the competent supervisory authority within 72 hours, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

9.23 Does LRQA have a designated data protection officer?

LRQA has a designated Data Protection Officer (DPO) to handle any data protection queries, the DPO can be reached at dataprotection@lrqa.com any time.

9.24 What is the availability of the EiQ Platform?

EiQ Platform is targeted to be available in give calendar year is >=99%. This excludes planned maintenance windows.

9.25 Where does EiQ Platform data host?

The EiQ platform is hosted on AWS in North Virginia region in USA.

9.26 What is the backup policy?

Daily database snapshot is configured; 14 copies will be kept in North Virigina. Daily database dump is configured; 14 copies will be kept in Ohio region for contingency.

9.27 What is the disaster recovery plan?

BCP and DR (Disaster Recovery) plan have been established, the DR plan is tested annually to ensure the Recovery Time Objective (RTO; 4 hours for critical applications) and Recovery Point Objective (RPO; 24 hours) are met.

10 EiQ platform support

10.1 What is the EiQ incident management process?

Alerts will be escalated to Operations, Network Infrastructure, and Security coverage. Employees are trained in security incident response processes, including communication channels and escalation paths. We manage incidents on a Service Management platform.

Priority levels, response times and estimated resolution times

Priority	First response time	Estimated resolution time	Issue examples
Critical The application is down, causing critical impact to business operations if not restored quickly; no workaround available.	Immediate	4 hours	• Production environment down
P1 - **Urgent** The application is accessible, but some major functionalities are not working causing impact to business operations.	1 business hour	3-5 business days	• Large number of assessments missing for many clients • Page breaks for any functionalities • Page loading indefinitely due to some API error - Unable to perform any action on that page# • Audit report download not working for many clients#
P2 - **High** The application is significantly degraded and or impacting significant aspects of business operations.	2-5 business hours	2 Weeks (10 business days)	• Assessment missing for a specific client • Mismatch in assessment services • Primary service missing or wrongly marked • Sentinel - No link to site scorecard • Filtering in a screen not working as expected# • Incorrect data - Calculation of score is incorrect# • Missing findings in an assessment# • Unable to export/import data# • Hide, Unhide and Merge factories not working# • Risk colour not displayed as expected#
P3 - **Medium** The application is noticeably impaired, but most business operations can continue.	2-5 business hours	More than 2 Weeks	• Data discrepancy between overview and Program Trend reports - Pivot Checklists data • Sentinel issues • Data inconsistency between screens • Client category filtering/value not displayed as expected
P4- **Low** The application is minimally impaired, without noticeable impact to business operations.	2-5 business hours	More than 2 Weeks	• Cosmetic issues^ - incorrect font, incorrect formatting, incorrect size of font • Design related issues • Application access • Feature Requests

#If the listed example only occurs for a particular client/particular site/particular assessment/particular screen, then this should be marked as a “Medium” priority.

^Cosmetic issues are mostly known issues which team is working on documenting and fixing it in one ticket. All cosmetic issue should adhere to the design as per the style guide.

10.2 What are the hours for IT support?

Our support hours are UTC 0100-1700, excluding Saturday, Sunday and public holidays.

10.3 What is the process for EiQ Platform feature enhancements?

In regular cadence, EiQ will have features and bug fixes deployed. Following a change approval process. Details of major features can be obtained by our Customer Success Team.

11 Understanding ESG risk data

11.1 EiQ relies heavily on audit data. What fields are measured as a part of a social and environmental audit?

A social and environmental audit evaluates a company's adherence to ethical, social, and environmental standards. A single audit may assess performance across as many as 400 different issues spanning labor, health & safety, environment, business ethics and management systems. Social and environmental audits are run by accredited professionals and may span from one to four days, depending upon the size of a production site. To see the structure of a typical audit, please click here.

11.2 What is inherent risk?

The risk associated with a region, activity, product or site in an unaltered state, without interventions or control mechanisms in place for mitigating risk. Inherent risk forms the basis of the ratings we offer as a part of EiQ's Risk Exposure module.

11.3 What is risk exposure vs risk management?

Risk exposure shows the inherent risk associated with a region, activity, product or site. Risk management reflects the risk associated with a site after risk control mechanisms are evaluated for their effectiveness in risk mitigation. These include any audits, grievance mechanisms or worker sentiment surveys that are undertaken as a part of your responsible sourcing practices.

11.4 How do I interpret the risk assignment given to a site through an evaluation of risk exposure versus risk management in analytics' segmentation module?

The risk treatment suggested for a site varies in accordance with its exposure to inherent risk versus managed risk. An extreme risk designation – high inherent risk, high managed risk – often requires a more stringent set of interventions – be it audits, grievance mechanisms or worker sentiment surveys. A site that is deemed to have a high degree of inherent risk but a low degree of managed risk or a high degree of managed risk, but a low degree of inherent risk may require less stringent intervention. The exact intervention, however, is often determined by the nature of the parent organization's business model.

11.5 What is supply chain ESG due diligence?

Supply chain due diligence is the process organizations use to identify, prevent, and mitigate the adverse impact of their entire supply chain operations, typically as it relates to environmental, social, and governance (ESG) issues. The key to achieving supply chain due diligence requires extending the risk mitigation process to suppliers and business partners further than just Tier-1 (or direct) suppliers, including third parties involved in the supply chain operations.

11.6 What is supply chain risk mapping?

Risk mapping is the process companies use to organize and illustrate an organization's supply chain risks. This is done by identifying and mapping information on each of the suppliers and individuals involved- from sourcing to procurement. Risk mapping is vital to achieving supply chain due diligence to reduce risks, meet regulatory requirements, and increase transparency for key stakeholders.