

Service Provider and Vendor Due Diligence Reviews

IQ-EQ offers independent service provider and vendor due diligence reviews designed to provide compliance officers with reporting that integrates into their compliance monitoring and satisfies the guidance and regulatory requirements of regulators in the UK, EU and the United States.

Each vendor due diligence review measures and assesses the vendor risk, financial health and data security best practices. To accomplish this, IQ-EQ employs a due diligence team comprised of experts in regulatory compliance, accounting & audit and IT.

The due diligence reviews and scope are customised to each organisation's needs, but include the following:

- Creation (or updating) of a service provider and vendor register;
- An internal risk assessment for each vendor;
- Sending and collection of questionnaires customised to your organisation's need;
- Review of documentation related to data protection, operational and financial controls
- Discussion with vendors related to financial health and growth of business; and
- Background checks and public search reviews.

The output of our due diligence is a collection of materials that easily integrate into a compliance monitoring programme and annual compliance review.

A report on each vendor reviewed is produced. Each report documents the risk rating, the assessment of the vendor and identifies any potential red flags and concerns. Our reports are designed as standalone documents to be shared with senior management, a board of directors or during a regulatory examination.

IQ-EQ Vendor Due Diligence Process

Our vendor due diligence process follows a standard outline that is easily customised to the circumstance and need of our clients.

A. Creation of a Service Provider and Vendor Register

Most regulators require or recommend that a catalogue or register be created to identify all service providers and third parties that have access to client or firm data.

The Service Provider and Vendor Register documents each third party, details the business function, business owner, whether the vendor has access or hosts client or firm data. Depending on the scope and coverage of the engagement, the due diligence reviews all vendors or selected vendors deemed higher risk.

B. The Internal Assessment and Risk Rating

The Internal Assessment and Risk Rating is developed in conjunction with the Register. In addition to identifying the risk related to the business function and purpose, we speak internally with product owners and day-to-day contacts to assess vendor performance and to understand and document where the individuals communicating with the service providers and vendors identify risk.

C. Service Provider and Vendor Questionnaire

Questionnaires are distributed to each vendor that is selected for review. Questionnaires can be customised for each engagement but generally include a review of:

- Cybersecurity and data protection controls
- Controls related to specific functions (e.g., AML controls, third party marketing)
- Operational and service changes
- Financial circumstance and change
- Documentation requests

D. Documentation Review

In conjunction with the questionnaire each vendor review requests and reviews documentation related to cybersecurity, accounting controls and any certification that the firm has undertaken. The documentation review includes review of SOC Reports, SSAE reports, AITECH Questionnaires, ISO Certifications, documentation related to AML and any other independent reviews.

E. Discussions with Vendors

If required and/or as a result of the questionnaire responses, a discussion and interview with the vendor can be undertaken. The discussions generally related to clarifications related to the service being provided, any noted changes in the vendor's financial circumstance and questions related to data protection controls.

F. Background and KYC Checks

Finally background and KYC checks are performed on the company and any key executives. These background checks include standard KYC reviews, web searches and regulatory searches (where applicable).

Due Diligence Report Production & Delivery

After the data has been collected and reviewed the information is compiled into a standalone due diligence report. The Report's Executive Summary provides a detail list of potential red flags and concerns that are raised against regulatory rules and best practice standards. The report content is divided into the following sections.

- Executive Summary and Overview
- Risk Rating
- Description of the Services Provide to the Firm
- Risk Assessment
- Cybersecurity and Data Protection Review
- Financial Stability Review
- Staffing and Servicing of the Firm

Report production takes approximately four to six weeks depending on the number of service provider and vendor reviews and the time it takes to collect questionnaire responses.

Key facts and figures*

People worldwide

4300⁺

Worldwide location

24

Assets under administration

\$750⁺ bn

Minimum senior team experience

20yrs

Funds under administration

800⁺

Key contacts



Edwin Chan

Chief Commercial Officer, UK & Ireland

E edwin.chan@iqeq.com

T +44 7510 369 485



George Wood

Managing Director

E george.wood@iqeq.com

T +1 410 227 2797

Our locations worldwide

THE AMERICAS

Bermuda
British Virgin Islands
Cayman Islands
Curaçao
USA (Austin, Bedford NH, Chicago, Dallas, Fort Worth, Garden City NY, Houston, Iselin NJ, New York City, Rapid City SD, San Francisco and West Palm Beach)*

EUROPE

Belgium
Cyprus
France
Guernsey
Ireland
Isle of Man
Jersey
Luxembourg
Switzerland
The Netherlands
UK

AFRICA

Mauritius
South Africa

ASIA

Mainland China (Shanghai & Shenzhen)
Hong Kong
India
Japan
Philippines
Singapore

*Information correct as of 30 January 2023

This document is provided for information purposes only and does not constitute legal, tax, investment, regulatory, accounting or other professional advice. For more information on the legal and regulatory status of IQ-EQ companies please visit www.iqeq.com/legal-and-compliance

Reference: MIS_439_30012023

© IQ-EQ 2023