Enterprise-Wide Risk Assessment Best Practice Checklist

FINTRAIL

Enterprise-Wide Risk Assessment: The essential pillar of your anti-financial crime framework

Your enterprise wide risk assessment (EWRA), also referred to as a 'business risk assessment', is the foundation of your anti-financial control (AFC) framework. It provides you with a holistic view of the financial crime risks and threats you face and informs the controls and systems needed to mitigate them.

The assessment should be much more than an annual tick box exercise, as done correctly it will deliver immense benefit to your organisation. Whilst not an audit, it is an opportunity to meaningfully review and improve your control framework. It provides a thorough assessment of the risks your business faces, and how effectively you are mitigating them. It is a powerful tool to identify the strengths and weaknesses of your programme - identifying issues means the process is working!

A robust EWRA also provides an opportunity to demonstrate your awareness of any deficiencies in your programme, and how and when you plan to address them. It is important to ensure you use its outputs to communicate to senior management where investment and resources are needed. And let's not forget, it's a minimum regulatory requirement of regulated firms.

The UK's Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 Section 18 states:

1. A relevant person must take appropriate steps to identify and assess the risks of money laundering and terrorist financing to which its business is subject.
2. In carrying out the risk assessment required under paragraph (1), a relevant person must take into account—
    a. information made available to them by the supervisory authority under regulations 17(9) and 47, and
    b. risk factors including factors relating to—
        i. its customers;
        ii. the countries or geographic areas in which it operates;
        iii. its products or services;
        iv. its transactions; and
        v. its delivery channels.

Section 18A notes that firms must also identify and assess the risks of proliferation financing to which its business is subject.

The European Banking Authority's Money Laundering/Terrorist Financing Risk Factors Guidelines' under Articles 17 and 18(4) of Directive (EU) 2015/849 state that:

1. Firms should ensure that they have a thorough understanding of the ML/TF risks to which they are exposed.
2. Firms should assess: the ML/TF risk to which they are exposed as a result of the nature and complexity of their business (the business-wide risk assessment);

So we've established the need for a robust, meaningful EWRA, but achieving this is often easier said than done. It can be difficult to know where to start, or what to include. FINTRAIL has created this best practice checklist to provide some critical questions you may wish to consider when conducting your EWRA. Please use the following areas as suggestions which should be tailored for your firm. The checklist should serve as a guide; it is not intended to be exhaustive or prescriptive. Depending on the size and complexity of your firm the details in this checklist may not be appropriate or necessary.

Preparation and scope

- ☐ Do you have a documented methodology that outlines your EWRA approach and process?
- ☐ Do you have a clear and documented view of how your risk appetite impacts your EWRA?
- ☐ Does your EWRA model cover the following areas?
  - ☐ Money laundering
  - ☐ Sanctions
  - ☐ Terrorist financing
  - ☐ Bribery and corruption
  - ☐ Proliferation financing
  - ☐ Fraud (internal and external)
  - ☐ Tax evasion
- ☐ Do you consider the following factors in your EWRA, as a minimum:
  - ☐ Product
  - ☐ Geography
  - ☐ Customer
  - ☐ Delivery channel
- ☐ If an area is not covered, do you document the rationale?
- ☐ Does your EWRA include threats and typologies identified internally through transaction monitoring, internal/external SARs, and when exiting clients for financial crime reasons?
- ☐ Does your EWRA incorporate trends identified through receipt of external production orders and requests for information from sources such as law enforcement and financial partners?

Inherent risks

- ☐ Does your EWRA include threats and typologies identified in the latest National Risk Assessment?
- ☐ Does your EWRA include threats and typologies highlighted by law enforcement?
- ☐ Does your EWRA factor in recent regulatory changes, issues raised in recent thematic reviews, and any other appropriate regulatory guidance?
- ☐ Does your EWRA incorporate both qualitative and quantitative data?
- ☐ Do you have a methodology that considers, as a minimum:
  - ☐ Likelihood of the risk occurring
  - ☐ Impact of the risk if it occurred

Control environment

- ☐ Are all your controls documented and compiled in a controls library?
- ☐ Do you map your controls to specific risk areas and/or scenarios?
- ☐ Do you assess the implementation and effectiveness of your controls?
- ☐ Do you consider outputs of an internal assurance programme and/or external audit when assessing effectiveness of your controls?

Residual risks

- ☐ Have you documented your residual risk calculation methodology?
- ☐ Do you assess if high residual risks are acceptable and what mitigation is needed if not?
- ☐ Do you have a documented risk threshold tolerance, and a process for mitigating or eliminating defined levels of risk?
- ☐ Do you assess the impact of your EWRA on your risk appetite and if it is aligned?
- ☐ Do you assign risk owners to various risk areas?
- ☐ Do you document clear action plans with timeframes for risks or controls with unsatisfactory effectiveness that are outside of your risk appetite?

Approval and implementation

- ☐ Do you communicate the output of the EWRA to the board and/or senior management and seek their approval of it?
- ☐ Do you work with the business to document, plan and execute the resulting action items?
- ☐ Can you demonstrate how your EWRA directly feeds into other controls e.g. customer risk assessments and transaction monitoring?
- ☐ Do you have a clear view of what effective implementation of the EWRA and the outputs and action plans looks like, with documented measures?

Keeping it dynamic

- ☐ Do you have clear and documented trigger events for EWRA review?
- ☐ Do you refresh your EWRA on the following occasions:
  - ☐ Entry to new markets
  - ☐ Launch of new products
  - ☐ New information on the external threat environment, e.g. a new National Risk Assessment
- ☐ Does your EWRA inform budget and resource allocation?
- ☐ Is your EWRA used in project prioritisation?
- ☐ When conducting horizon scanning do you consider the impact on your EWRA?

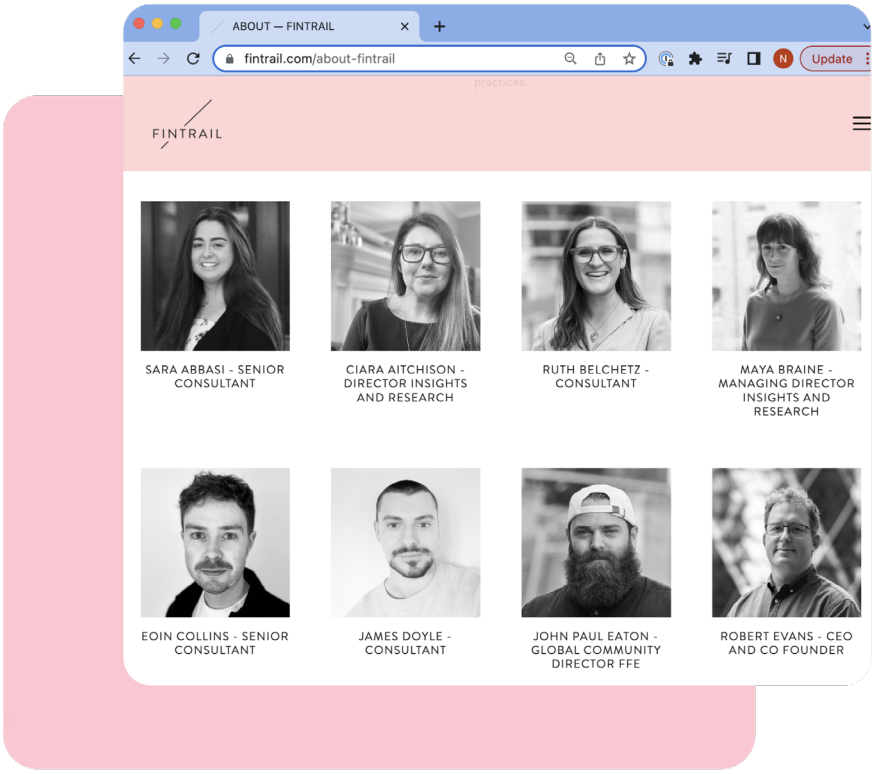
About FINTRAIL

At FINTRAIL we are passionate about combating financial crime. Our unique team of experts is drawn from the industries we support and has deep hands-on experience in developing and deploying risk management controls from leadership roles with leading banks, FinTechs, and other financial institutions.

We have extensive experience assisting financial services businesses with building and conducting their EWRA. We have a proven track record of identifying areas where clients can enhance their compliance and make their programmes more effective.

Our approach is tailored to the unique circumstances of each client, is regulatory and technology driven, and is focused on providing excellent customer outcomes. We offer our clients pragmatic solutions to the most complex challenges and our goal is to ensure our clients can thrive, free from the negative impacts of financial crime.

If you wish to speak to our team about your requirements for conducting or reviewing your EWRA please get in touch with us.



Find out more about our services

www.fintrail.com
contact@fintrail.com