Executive summary
This document defines the key elements of the Legal & General Group’s (“L&G” or “the Group”) financial crime risk management framework setting out the policy requirements and minimum control standards.
Senior managers, especially those with explicit financial crime risk management roles, must consider these policy requirements and control standards when designing and operating their systems and controls.

Contents

1 About this document .......................................................................................................................... 2
1.1 Target audience ............................................................................................................................... 2
1.2 Scope ............................................................................................................................................... 2
1.3 Relevant laws and regulations ........................................................................................................ 2
1.4 Policy statement ............................................................................................................................. 3
1.5 Documentation retention requirements .......................................................................................... 4
1.6 Obtaining policy waivers and exemptions .................................................................................... 4
1.7 Reporting breaches of policy .......................................................................................................... 4
1.8 Process for gaining assurance of compliance ................................................................................ 4

2 Financial crime risk framework ...................................................................................................... 5
2.1 Risk assessment .............................................................................................................................. 5
2.1.1 Maintain a risk assessment .......................................................................................................... 5
2.2 Due diligence .................................................................................................................................. 5
2.2.1 Determine the level of due diligence .......................................................................................... 5
2.2.2 Initial due diligence .................................................................................................................... 5
2.2.3 Ongoing due diligence ................................................................................................................ 6
2.2.4 Special categories ....................................................................................................................... 6
2.3 Screening ........................................................................................................................................ 6
2.3.1 Determine the screening programme .......................................................................................... 7
2.3.2 Conduct the screening programme .............................................................................................. 7
2.4 Monitoring for unusual behaviour or activity ................................................................................ 7
2.4.1 Determine the level of activity monitoring ................................................................................. 7
2.4.2 Conduct the monitoring programme ........................................................................................... 8
2.5 Reporting a suspicion ...................................................................................................................... 8
2.6 Staff vetting and training ............................................................................................................... 8

3 Roles & responsibilities .................................................................................................................... 9
3.1 All staff .......................................................................................................................................... 9
3.2 Senior management ....................................................................................................................... 9
3.3 Fraud specialists ............................................................................................................................. 9
3.4 Money Laundering Reporting Officer ............................................................................................ 9
3.5 Operating division risk teams (divisional second line) ................................................................. 10
3.6 Group Financial Crime (Group second line) ................................................................................ 10
1 About this document

This document defines the key elements of the Legal & General Group’s ("L&G" or "the Group") financial crime risk management framework setting out the policy requirements and minimum control standards. It should be read in conjunction with relevant Groupwide Technical Guidance. For the avoidance of doubt where additional, subsidiary, Policies and Standards are introduced to meet the requirements of this policy, if there is any conflict this policy takes precedence.

1.1 Target audience

This document is intended for all managers across the Group, particularly those responsible for the design and operation of financial crime internal systems and controls, as well as Group and Divisional Chief Risk Officer (CRO) teams responsible for oversight of those internal systems and controls.

1.2 Scope

The policy applies to all activities undertaken in support of L&G’s strategic objectives by, or on behalf of, all firms consolidated within the Group’s statutory accounts. Where L&G’s ability to control/direct the subsidiary is constrained by external investors we will expect a comparable policy to apply. Within the context of this Policy, financial crime is defined as:

- Money Laundering
- Terrorist Financing
- Fraud (Internal & External)
- Bribery & Corruption
- Insider Dealing
- Market Manipulation; and
- Facilitation of Tax Evasion

1.3 Relevant laws and regulations

The key legislative and regulatory influences on this policy are listed below:

<table>
<thead>
<tr>
<th>Policy Scope</th>
<th>Relevant laws and regulations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud</td>
<td>The Fraud Act 2006, came into effect on 15 January 2007, it gives a statutory definition of the criminal offence of fraud. It requires that, for an offence to have occurred, the person must have acted dishonestly, and that they had to have acted with the intent of making a gain for themselves or anyone else, or inflicting a loss (or a risk of loss) on another.</td>
</tr>
<tr>
<td>Bribery</td>
<td>The Bribery Act 2010 covers the criminal law relating to bribery. The Act came into force on 1 July 2011, and covers the crimes of bribery, being bribed, the bribery of foreign public officials, and the failure of a commercial organisation to prevent bribery on its behalf. The Act has a near-universal jurisdiction, allowing for the prosecution of an individual or company with links to the United Kingdom, regardless of where the crime occurred.</td>
</tr>
<tr>
<td>Insider Dealing &amp; Market Manipulation</td>
<td>Insider dealing is a criminal offence under section 52 of the Criminal Justice Act 1993. Sections 89-91 of the Financial Services Act 2012 set out a range of behaviours which amount to criminal offences, which are together referred to as market manipulation.</td>
</tr>
<tr>
<td>Facilitation of Tax Evasion</td>
<td>The Criminal Finances Act 2017 (which amends POCA) came into effect on 30 September 2017. The Act makes companies and partnerships criminally liable if they fail to prevent tax evasion by either a member of their staff or an external agent, even where the business was not involved in the act, or was unaware of it.</td>
</tr>
<tr>
<td>All</td>
<td>The FCA’s Financial Crime Guide for Firms (the Guide) consolidates their guidance on financial crime and aims to enhance firms’ understanding of their expectations of systems and controls in this area. The Guide provides practical assistance and information for firms of all sizes on actions they can take to counter the risk that they might be used to further financial crime.</td>
</tr>
</tbody>
</table>
1.4 Policy statement

It is the Group’s policy that the following steps are taken to manage the Group’s exposure to financial crime risk:

1. **Business activity** – operating divisions, or any person acting on their behalf, must not enter into any activity that would result in financial crime, nor may they enter into any activity that would enable others in committing a financial crime.

2. **Risk assessment** – each operating division must ensure that a current assessment of the financial crime risk is maintained and available to senior managers, and that the divisional risk appetites and tolerances are documented and approved in line with the Group’s Risk Appetite Statement.

3. **Systems and controls** – each operating division must design and implement proportionate systems and controls to manage their activities (taking account of the current risk assessment, appetite and tolerances).

4. **Due diligence** – where operating divisions enter into a business relationship (including one off transactions) with another party, they must undertake an appropriate due diligence assessment of the risk presented by the business relationship, and define periodic re-assessments of that risk.

5. **Screening** – either prior to, or within a short period, each operating division must take steps to identify whether any party with whom they have a business relationship is subject to financial sanctions (or performs a prominent public role) and to assess the risk presented by any such business relationship.

6. **Staff awareness and training** – senior managers must ensure that relevant staff are aware of their obligations in relation to financial crime, most significantly their obligation to report any suspicious activity, and ensure more targeted training is provided and assessed for those occupying relevant roles.

7. **Monitoring for unusual activity** – each operating division must put in place monitoring, appropriate to the financial crime risk presented, to demonstrate adherence to this policy and/or to identify any suspicious activity that requires investigation.

8. **Suspicious activity** – where an individual identifies any knowledge or suspicion of a financial crime they must immediately report it to the operating division’s nominated person designated to receive such reports. That nominated person, or their deputy, must investigate the concern and, if required, disclose the matter to external law enforcement and/or regulatory authorities.
1.5 Documentation retention requirements

Personal data obtained to comply with this policy must only be processed for the purposes of preventing financial crime; no other use may be made of the data, unless permitted under other law, or the party to whom the data relates provides their consent. Each operating division must provide new customers and other relevant parties with notification of the above.

<table>
<thead>
<tr>
<th>Due Diligence</th>
<th>Records of the due diligence undertaken for relevant parties, including senior manager approval for high risk relationships, must be retained for 5 years from the date the relationship ends.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screening</td>
<td>Records of screening results must be retained for 5 years from the date of screening and (for identified higher risk parties) for 5 years from the date the relationship ends.</td>
</tr>
<tr>
<td>Staff Vetting</td>
<td>Records of vetting must be retained for 7 years from the end of the employment.</td>
</tr>
<tr>
<td>Transactions</td>
<td>Records of transactions must be retained for 5 years from the date of any single transaction, or 5 years from the date the relationship ends for continuous relationships (up to a maximum of 10 years from the date of the transaction).</td>
</tr>
<tr>
<td>Trusts</td>
<td>For operating divisions acting as Trustee, or undertaking administration under trust, records of beneficial owners must be maintained and retained for 5 years after the final distribution under the Trust.</td>
</tr>
<tr>
<td>Suspicious Activity Reports</td>
<td>Records of applicable information must be retained for 5 years from the report, or for 5 years after the investigation is closed by external authorities when a disclosure is made.</td>
</tr>
</tbody>
</table>

Once the retention period has expired, the personal data obtained for the purposes of this policy must be deleted, unless there is a valid reason to retain the data past the specified retention period, as follows:

- A legislative or relevant regulatory requirement;
- For the purposes of any court proceedings;
- There are reasonable grounds to believe that the data needs to be retained for legal proceedings; or
- The party, to whom the data relates, provides their consent.

1.6 Obtaining policy waivers and exemptions

Operating divisions are expected to comply with this policy. Managers seeking policy waivers or exemptions should contact the Policy Owner stating exactly what is required (including relevant time periods and other limitations) and providing justification. Approval may be granted in exceptional circumstances and must be provided prior to any deliberate policy breach.

Where managers seek to accept a level of risk outside of the risk appetite approval should be sought from the relevant second line manager responsible for financial crime oversight prior to seeking approval through the relevant operating division management committee. Risk acceptance must be recorded on the appropriate risk management system (e.g. OneSumX).

1.7 Reporting breaches of policy

All breaches of this policy must be reported to the Policy Owner as soon as they are identified. The Policy Owner will agree the appropriate action and reporting.

1.8 Process for gaining assurance of compliance

The Policy Owner will seek assurance of compliance with this policy by completion of the annual Risk Framework Review and oversight of:

- Group-wide control attestation process, risk issues and risk events raised on risk register;
- Operating divisions financial crime risk assessments;
- MI showing the status of key control metrics;
- Material concerns raised through audit and compliance review activity;
- Surveillance of operating divisions to identify shifts in financial crime risk profiles; and
- Reporting to operating divisions and Group-wide risk committees.

The Policy Owner will escalate identified areas of non-compliance as appropriate, and provide a certificate of policy operation and compliance/exceptions as part of the annual Risk Framework Review.
2 Financial crime risk framework

In order to meet the policy statements, the following framework must be adopted:

2.1 Risk assessment

In order to design risk based processes to manage their financial crime risk, operating division senior management must have a current and detailed understanding of the risks posed through their products and services.

2.1.1 Maintain a risk assessment

Senior managers within each operating division must maintain an assessment of their financial crime risks and ensure this assessment is considered and accepted through relevant risk governance framework no less frequently than annually.

2.2 Due diligence

In order to understand the financial crime risk presented by an individual business relationship, an operating division must conduct sufficient due diligence at outset and at other appropriate trigger points during the business relationship.

2.2.1 Determine the level of due diligence

Operating divisions must determine the level of due diligence to be undertaken based upon the risk assessment undertaken to meet 2.1.1 of this policy. This determination includes:

- Identification – sufficient information must be obtained to uniquely identify the parties to the business relationship including, where applicable, the beneficial owners.
- Verification of Identity – on the basis of documentation, data or information obtained from an independent source, the identity of the parties to the business relationship must be verified.
- Purpose and nature – the purpose and nature of the relationship must be understood. (For the majority of business relationships this would be a general understanding of the purpose and nature of the product or service involved in the business relationship).
- Source/destination bank account – the originating or recipient bank account for all transactions must be identified and recorded.

2.2.2 Initial due diligence

Operating divisions must undertake initial due diligence prior to the establishment of a business relationship unless it is necessary to complete initial due diligence during the establishment of the business relationship, so as not to interrupt the conduct of business, provided the product/service risk has been determined as ‘low’ under 2.1.1 of this policy.

If operating divisions are not able to complete the initial due diligence, they must not enter into, or continue, with the business relationship and consider if the circumstances should be reported as a suspicious activity. Any return of funds must be made to the originating account.

If the risk of the individual business relationship is assessed as ‘high’, operating divisions must undertake enhanced due diligence, including an assessment of some, or all, of the following:

- Source of funds – the origins of the funds involved in the business relationship or occasional transaction (e.g. the activity that generated the funds or how the funds were accumulated).
- Source of wealth – the origins of the party’s total wealth (e.g. how they acquired their total assets).
- Business or professional activities - where the business relationship is with an entity, an assessment of the activities undertaken by that entity.

Based upon the assessment of financial crime risk from this initial due diligence, operating divisions must set the level of monitoring required during the period of the business relationship (for the majority of business relationship this will be determined by the product/service risk assessment under 2.1.1 of this policy).
2.2.3 Ongoing due diligence

**Operating divisions must undertake ongoing due diligence** at trigger points during the lifetime of the business relationship based upon the assessment of financial crime risk of the individual business relationship.

In determining the trigger points when ongoing due diligence is required, operating divisions should consider the overall assessment of financial crime risk for the product/service and recognise changes to the risk of the individual business relationship, including:

- **Change of identity** – when the identity of the party, or its beneficial owner, to the business relationship changes.
- **Doubt the original documentation** – when there is any doubt about the validity of the original documents.
- **Atypical activity** – when an activity takes place that is not in line with the anticipated purpose and nature of the relationship.
- **Change of jurisdiction risk** – where the party to the business relationship moves to a jurisdiction with a different risk level.
- **Sanctions or Politically Exposed Persons** – when the party to the business relationship becomes, or ceases to be, subject to financial sanction or in a prominent public role.

2.2.4 Special categories

**Correspondent relationships** - where an operating division wishes to establish a correspondent relationship with another credit or financial institution in a country that is outside the EEA, this must be approved by the division’s senior management and the relevant firm’s MLRO. The requirements of the UK’s Money Laundering Regulations 2017 (Regulation 34) must be considered prior to declining or granting approval to proceed.

Business relationships must not be entered into or continued with a shell bank. Operating divisions must also take appropriate measures to ensure that they do not engage in or continue relationships with a bank, credit or financial institution that is known to allow its accounts to be used by a shell bank.

**Social Inclusion** - operating divisions must ensure they do not exclude customers who have a legitimate social reason for not being able to provide the standard forms of evidence of identity, and should find suitable alternative means of identifying and verifying the customer.

2.3 Screening

Financial sanctions are periodically issued against entities and individuals by relevant regulatory bodies in each jurisdiction that the Group operates in. Under these financial sanction regulations, firms must not enter into, or maintain, a business relationship with a sanctioned party without licence from the relevant regulatory body.

It is a regulatory requirement to identify business relationships with parties, including beneficial owners, who are in a prominent public role (referred to as politically exposed persons) and to consider whether that role and the nature of our business relationship represents an elevated risk requiring additional controls and monitoring.

Firms are also required to have in place systems and controls to prevent their products/services being used to fund terrorism, facilitate financial crime, or for holding the proceeds of crime. If firms suspect their products/services are being used for such a purpose, they must disclose the matter to the relevant regulatory authorities within their jurisdiction.

In order to meet these requirements, operating divisions must establish and maintain a screening programme to identify parties, with whom they have a business relationship, who are either sanctioned, politically exposed, or where there is suspicion of the funding or terrorism or involving the proceeds of crime.
2.3.1 Determine the screening programme

Operating divisions must determine and document the screening programme relevant to their operations, taking account of the product/service risk assessment under 2.1.1 of this policy, which must include:

- **Parties to screen** – identify those parties that must be screened, including customers, suppliers, distributors, partners, employees, and contractors.
- **Screening criteria** – the sanction lists (which must include the UN, EU, UK and US(OFAC) regimes); the definition of prominent public role; and the rules to be applied to identify potential matches.
- **Timing of screening** – for each party, the timing and frequency of screening.

2.3.2 Conduct the screening programme

🔒 Operating divisions must conduct a screening programme as specified under 2.3.1 of this policy.

When the screening programme confirms that a party to a business relationship matches a sanctioned person the operating division’s Money Laundering Reporting Officer (MLRO) and the division’s senior management must consider the risk presented by the relationship and notify the relevant authorities. Where a sanction order applies operating divisions must not make payments unless the relevant authority has provided a licence to proceed.

When the screening programme confirms that a party to a business relationship matches a person in a prominent public role (PEP), the operating division’s MLRO must assess the risk presented by the relationship:

- **High risk** – Where the relationship is considered high risk, they must recommend to the operating division’s senior management whether the business relationship should proceed/continue and the operating division’s senior management must consider and approve or reject this recommendation.
- **Former PEP** – When a party to the business relationship ceases to be in a prominent public role the operating division must consider the risk presented by the business relationship for a further period of 12 months.

When the screening programme identifies a suspicion of terrorist financing or holding the proceeds of crime, the operating division’s MLRO must consider the risk, and whether a notification to relevant authorities is required.

2.4 Monitoring for unusual behaviour or activity

Periodic monitoring of transactions and activities associated with each business relationship to identify and investigate suspicious activity enables operating divisions to detect and prevent financial crime. Typically, an understanding of the anticipated nature of the business relationship exists from the risk assessment in 2.1.1 of this policy, and monitoring is put in place to identify variances from that anticipated behaviour with such variances investigated to establish whether any knowledge or suspicion of financial crime exists.

2.4.1 Determine the level of activity monitoring

Operating divisions must maintain monitoring indicators that will identify unusual activity by a party to a business relationship to suggest potential financial crime. Such monitoring should consider:

- **Money laundering risk** – consideration of transactions/activity that may be part of an attempt to disguise the proceeds of crime.
- **Bribery & corruption risk** – passive or active bribery or corruption that may induce a party to perform their function or activity improperly.
- **Market misconduct** – consider the transactions and behaviours that might result in insider dealing or market manipulate on.
- **Facilitation of tax evasion risk** – activity that may enable a party to evade tax.
- **Fraud risk** – consideration of transactions/activity that may be part of an attempt to defraud either the firm or the parties to the business relationship.
2.4.2 Conduct the monitoring programme

- Operating divisions must conduct monitoring for unusual activity as specified under 2.4.1 of this policy.

Unusual activity identified through monitoring must be investigated promptly, and any suspicion or knowledge of financial crime must be reported immediately to the operating division’s financial crime investigation team.

2.5 Reporting a suspicion

During the course of their duties, staff may become aware (or have suspicion) of a financial crime that has taken place, or may take place. It is beholden upon all individuals to report their suspicion to enable appropriate investigation and action to be undertaken.

- Staff must identify suspicious activity once they have knowledge (or suspicion) of a financial crime; they must report it immediately to the operating division’s financial crime investigation team.
- Where a transaction is pending at the time of making an internal report, this transaction must not proceed until advice has been received from the operating division’s financial crime investigation team.
- When an internal report has been made, staff must not alert the party to whom the internal report relates, or representatives of the party, that a report has been made unless advice has been received from the operating division’s financial crime investigation team.
- Any member of staff who reports a suspicion in good faith must not suffer detriment as a result of making such a report.
- All internal reports must be investigated promptly by the operating division’s financial crime investigation team and, if suspicion cannot be adequately allayed, it must be reported to the relevant authorities.

2.6 Staff vetting and training

Significant reliance is placed upon individual members of staff to detect and prevent financial crime; it is essential, therefore, that they are suitably vetted for their role and receive the relevant and necessary training.

- Operating divisions must determine and document the vetting and training standards required for all roles that exist within their division, which must include:
  - Pre-employment vetting – establishing the pre-employment vetting necessary to determine the degree of financial crime risk, including the risk of the individual committing or facilitating financial crime.
  - Ongoing vetting – establishing which roles require ongoing vetting, and determine the extent of that vetting, to maintain an assessment of the risk of financial crime, including the risk of the individual committing or facilitating financial crime.
  - Awareness training – all staff must receive a level of awareness training to understand financial crime risk and their responsibility to detect and prevent financial crime:
    - For new staff, this awareness training must take place no later than 30 days after they joined the company, and prior to them processing any financial transactions.
    - This awareness training must be repeated no less than annually thereafter.
  - Targeted training – establishing if any member of staff, or group of members of staff, requires additional targeted training in respect of financial crime risk pertinent to their role.

- Operating divisions must then conduct the pre-employment and ongoing vetting of staff.

- Operating divisions must complete the awareness and targeted financial crime risk training and take appropriate action when this is not completed in the required timescales.
3 Roles & responsibilities

The Group Risk Management Policy outlines L&G’s three line of defence risk management model. The respective roles and responsibilities of the key stakeholders to the effectiveness of this policy are set out below:

3.1 All staff

All staff must complete their training in the timescale directed by their senior management, and must report any knowledge, or suspicion, of financial crime to their operating division’s financial crime investigation team.

3.2 Senior management

Senior management have a responsibility to ensure that this policy is fully implemented in Group companies and that proportionate systems and controls are working effectively. This includes activities that are outsourced. In particular, senior management must:

- **Understand their financial crime risks** – have a clear and documented understanding of the financial crime risks pertinent to their operating division and have determined their operating division’s appetite for these risks.
- **Implement internal controls** – in line with the operating division’s understanding and appetite for financial crime risks to implement and document effective procedures and controls to prevent and detect financial crime.
- **Staff training** – provide suitable training to their staff to enable them to perform their duties and obligations to prevent and detect financial crime.
- **Monitor and review** – implement relevant and timely monitoring to measure the effectiveness of the internal controls and (where they are operating outside of appetite) to take appropriate action to return to operating within risk appetite.
- **Screening** – ensure screening of relevant parties is undertaken, and consider the financial crime risks of high-risk parties, taking account of the recommendations of the operating division’s financial crime team, prior to any approval to accept, retain, or decline a relationship with them.

3.3 Fraud specialists

Operating divisions may establish specialist fraud investigation roles to support senior management in the prevention and detection of fraud risks encountered in the normal course of their business, such as claims frauds, or application frauds. These specialists may sit within the first line or the second line of defence, and are responsible for the investigation of suspected fraudulent activity to prevent or mitigate the effect of such activity.

3.4 Money Laundering Reporting Officer

Operating divisions must appoint a nominated officer who is responsible for receiving disclosures of money laundering or terrorist financing, and deciding whether these should be reported to external law enforcement agencies, and, if appropriate, making such external reports. This officer, referred to here as the Money Laundering Reporting Officer (MLRO):

- Should know about the money laundering and terrorist financing risks to the operating division they are appointed to oversee and make sure steps are taken to mitigate those risks effectively;
- Must have the authority to act independently in carrying out their responsibilities, and be able to liaise with the regulator and law enforcement directly; and
- Should provide an annual report on the effectiveness of the control environment to the Board of any firm that is covered by the UK Money Laundering Regulations, and may choose to provide similar reports to any other firm within the Group.

The MLRO’s responsibility may be delegated, providing the delegate is notified in writing with the clearly defined areas of authority. This must state their nominated officer responsibilities, under which legislation, for which operating division, and specify that they are authorised to investigate suspicious activity and have the authority to make onward suspicious activity reports to the relevant authority.
3.5 Operating division risk teams (divisional second line)

The second line of defence has been established to provide business management with support and oversight of operational and conduct risks. In the context of financial crime, these teams are required to recognise and identify changes in the financial crime risk profile and environment, and are responsible for:

- **Business management support** – provide support to management in control design and implementation which may include specific financial crime guidance to enable business management to meet the obligations of this policy.
- **Evaluation** – evaluate the appropriateness of the financial crime control framework and the effectiveness of its operation.
- **Oversight** – oversee compliance with regulatory and legislative standards.
- **Deficiencies** – assess and report on material deficiencies.
- **Verification** – verify control attestations and challenge if necessary.

3.6 Group Financial Crime (Group second line)

Legal & General Group has established a Group Financial Crime function who are responsible for:

- **Policy** - set the Group level policy and minimum standards
- **Business management support** – provide support to operating division’s management, financial crime specialists and divisional risk teams in control design and implementation which may include specific financial crime guidance to enable business management meet the obligations of this policy.
- **Evaluation** – evaluate the appropriateness of the financial crime control framework within the operating divisions and the effectiveness of its operation.
- **Oversight and challenge** – receive reports from operating divisions to oversee compliance with relevant regulatory and legislative standards, and challenge any matter that will affect that compliance.
- **Deficiencies** – assess and report on material deficiencies, especially those that exist across operating divisions.
- **Information sharing** – establish and maintain (throughout the Group) procedures for sharing information for the purposes of preventing and detecting financial crime.