1. Introduction

1.1. Purpose & Scope

This policy sets out Control Standards (CS) for the management of Financial Crime / Fraud risks. It covers all aspects of Financial Crime / Fraud Risk within Countrywide and applies to all Group businesses, employees and contractors. Where local standards / regulation exceed the policy and control standards then they apply.

1.2. Guiding Principles

This policy is based on the following core principles:

- The interests of shareholders and other stakeholders are protected by ensuring that excessive powers are not delegated to individuals;
- Decisions taken by management are consistent with the ' CE } ps %ra[tegic objectives and are approved by the Board;
- Managers are accountable for the management of risk, including internal controls, in their business;
- Business is conducted in line with authorities and accountabilities ultimately delegated by the Board, these are described within specific policies;
- Clear accountabilities are delegated by management to employees with the right skills and competence; and
- Every member of staff is responsible for understanding and managing the risk they take on behalf of the Group and for ensuring that they act within the authorities and accountabilities delegated to them.

1.3. Review Process

This document is regularly reviewed by the Group Policy Owner to ensure continuing alignment with legal and regulatory requirements and business needs.

1.4. Financial Crime and Fraud Risk

A risk can be defined as something which may or may not happen (i.e. the possibility of an uncertain outcome), which if it did, could lead expected outcomes to vary, and where that became a negative outcome would result in an adverse impact on the achievement of business objectives.

Financial crime is defined as any kind of criminal conduct relating to money, assets, financial services and financial markets. It includes any offences involving fraud or dishonesty or misconduct in, or misuse of information relating to, a financial market; failing to prevent the facilitation of tax evasion; or handling the proceeds of crime

Fraud is defined as:

- Misappropriating, concealing, diverting or obtaining money, assets, information or services by deceptive means; and

- Misusing } v s[position through unlawful or improper acts intended to cause financial loss to Countrywide, its customers or suppliers.

Examples of Fraud would include:

- Fraudulent financial reporting;
- Criminal misrepresentation or impersonation;
- Falsifying documents;
- Misappropriating company assets or property; and
- Other defined as fraud under applicable laws.

The cost and negative consequences of financial crime and fraud include financial loss, management time, loss of trust in the Group, investigation costs, litigation and negative effects on reputation and employee morale. The Group has a zero r š } anceEapproach to financial crime and fraud.

1.5. Financial Crime and Fraud Risk Management Principles

The Group seeks to manage its exposure to financial crime and fraud risk by establishing principles and control standards. Key risk management principles for financial crime and fraud are included in the table below:

Risk Area	Principles
Organisation and Resources	Governance arrangements for management of financial crime / fraud are effective. The business has suitable resource to identify and manage its exposure to financial crime / fraud.
Financial Crime	Governance arrangements for the prevention, detection and reporting tax evasion. The business has suitable resource to identify and manage its exposure to financial crime.
Risk Assessment	The business has thoroughly assessed the risks of its products and services to financial crime / fraud. It has effective controls in place t mitigate these risks to an acceptable level.
Customer Due Diligence (CDD) and Politically Exposed Persons (PEPs)	The business has effective processes to collect, maintain and refresh relevant CDD and PEP relationships information.
Client Money	Client money is clearly segregated from business money and protected effectively as required by legislation and regulatory requirements.
Employee Dishonesty	Employee dishonesty is managed effectively.
Anti-bribery & corruption	The integrity of the business is maintained in the management of gifts and hospitality. The risk of bribery and corruption is managed and mitigated as required by legislation and regulation.
Training & awareness	Relevant employees understand their roles and responsibilities for financial crime / fraud and complete mandatory training as required

2. Contrd Standards

2.1. Minimum Control Standards

A Contrd Standard is an activity which must be in place in order to manage the risk areas defined in the table below. A minimum set of control standards, covering a range of directive, preventative, detective, corrective and limiting controls ensure that, where they operate effectively, risk is managed to an acceptable level.

Group functions and Business Units need to demonstrate compliance with the minimum control standards (MCS) set out in the table below:

Risk Area	Risk Definition	MCS
Organisation and resources	Loss arising from a failure to manage fraud risks effectively.	• Senior management is engaged in the management of financial crime / fraud risks • The business is organised and resourced to ensure legal and regulatory compliance with financial crime / fraud requirements • All employees in the business are fully aware of their financial crime / fraud accountabilities / responsibilities. • The business processes to manage financial crime / fraud are documented and understood by employees • Effective reporting is provided to senior management covering financial crime / fraud investigations, losses and controls • Financial crime / Fraud breaches are reported in a timely manner and serious concerns are escalated to the Enterprise Risk Director or Group Head of Legal
Financial Crime	Loss arising from a failure to prevent, detect and report tax evasion.	• A thorough review of the businesses risks and associated processes and procedures to ensure that all appropriate steps are taken to prevent facilitation of tax evasion. • Management of financial crime is appropriately prioritised by and transparent to employees *** see Table 1.0 which outlines possible red flags and mitigation.**
Risk Assessment	Loss arising from a failure to identify vulnerablities and prioritise mitigation.	• A thorough risk assessment of the businesse exposure to financial crime / fraud has been undertaken • Management of financial crime / fraud is appropriately prioritised by and transparent to employees

CDD and PEPs
.
	Loss arising from failure of employees to carry r } µ š appropriate customer due diligence checks.	• Effective CDD processes are in place for new relationships (including acceptable documentation, r] v š] (] & š] } verification tools etc.).
		• Effective processes are in place:
		  • To identify new and existing PEPs.
		  • For ongoing monitoring for high risk relationships.
		  • To highlight and report potentially suspicious transactions.

Client Money	Loss arising from a failure to protect client money.	• The business has effective processes in place to segregate client money from business money • Effective oversight is provided in the business to ensure that risks related to client money are effectively mitigated

Risk Area	Risk Definition	MCS

Anti-bribery & corruption	Loss arising from bribery and corruption of employees.	• Documented procedures and arrangements are in place for the:
		  • Effective management of risks relating to gifts and hospitality,
		  • Claims of costs related to travel and expenses
		  • Payments
		  • Procurement and supplier management
		  • Other aspects which could pose risks related to the bribery and corruption of employees in the business.

Employee Dishonesty	Loss arising from dishonest acts of employees.	• The risk of employee dishonesty is acknowledged and acted upon • Employees understand their obligations to act with integrity • New recruits are vetted per Countrywide requirements. • All cases of actual or suspected employee dishonesty are referred to š Z u ‰ o } Ç Z o š] } v e f o r e d a n y a c t i o n i s Ž a k e n.

Training and awareness	Loss arising from a failure to train employees in obligations to report financial crime/fraud	• Effective financial crime / fraud training is delivered regularly on:
		  • Relevant legislation covering aspects such as money laundering proceeds of financial crime, terrorist financing and bribery and corruption
		  • Fraud
		• Training materials are kept up to date including changes to related regulations and legislation

Table 1.0 – Financial Crime

The following is a list of possible red flags that may arise during the course of you working for us and which may raise concerns related to tax evasion or foreign tax evasion. The list is not intended to be exhaustive and is for illustrative purposes only:

Red Flags	**Mitigation Action**
As part of a property transaction you are asked to refer a client to a stamp duty advisory firm with the express intention of assisting the client to evade SDLT.	**Advise employees not to promote any tax avoidance schemes.**
You are asked, or initiate, structuring a property transaction in a way to evade SDLT.	**Advise employees not to promote any tax avoidance schemes.**
A landlord you know to be based overseas asks us to misrepresent their residence status to operate outside of the Non Resident Landlord Scheme receiving rent gross of tax.	**Our Terms of Business advise of the requirement. Employees are trained to be wary of circumstances where they believe the landlord is not residing in the UK and so requires an NRL number to receive rent gross.**
A landlord asks us to defer transfer of rent until the start of the new tax year in order to reduce their tax liability in the current year.	**Advise employees not to promote any tax avoidance schemes.**
A property owned in joint names is presented as being owned in the sole name of the lower tax payer, to reduce their overall tax liability.	**Terms of business warrant that the "landlord" is the beneficial owner. Duty to report any "reasonable suspicions".**
You provide a low property valuation either in error or knowingly to avoid capital gains or inheritance tax.	**Ensure valuations are carried out by suitably trained and mandated colleagues with robust peer review and audit processes in place.**
A third party requests payment in cash and/or refuses to sign a formal commission or fee agreement, or to provide an invoice or receipt for a payment made.	**All suppliers must agree to Countrywide's terms of business and will only be paid on presentation of a valid invoice.**
You become aware, in the course of your work, that a third party working for us as an employee asks to be	**All employees must be paid through payroll for all work undertaken.**

treated as a self-employed contractor, but without any material changes to their working conditions.	
A third party to whom we have provided services requests that their invoice is addressed to a different entity, where we did not provide services to such entity directly.	**All services must be invoiced to the correct contracting party.**
A third party to whom we have provided services asks us to change the description of services rendered on an invoice in a way that seems designed to obscure the nature of the services provided.	**All services must be invoiced accurately.**
You receive an invoice from a third party that appears to be non-standard or customised.	**A valid invoice must be presented.**
You notice that we have been invoiced for a commission or fee payment that appears too large or too small, given the service stated to have been provided.	**All invoices to be approved by line managers that can validate the invoice.**
You become aware, in the course of your work, that a third party has made or intends to make a false statement relating to tax, has failed to disclose income or gains to, or to register with, HMRC, has delivered or intends to deliver a false document relating to tax, or has set up or intends to set up a structure to try to hide income, gains or assets from a tax authority.	**Agree escalation process to HMRC with the Group Tax Manager. Duty to report any "reasonable suspicions".**
You become aware, in the course of your work, that a third party has deliberately failed to register for VAT or failed to account for VAT.	**Agree escalation process to HMRC with the Group Tax Manager. Duty to report any "reasonable suspicions".**
A third party requests or requires the use of an agent, intermediary, consultant, distributor or supplier that is not typically used by or known to us.	**Escalate to line manager for further investigation.**

2.2. Applying for policy waivers

In the event that areas of the business are not compliant with the above Control Standards a waiver from the policy may be provided by the Group / BU Policy Owner via Country wise governance arrangements. This will include the Policy Owner providing details of gaps in compliance and planned actions and timelines to address these.

3. Responsibilities

3.1. Group Policy Owner

The Countrywide Group Chief Financial Officer is the Group Policy Owner (GPO) and is accountable to the Countrywide Group Executive Committee for the design, implementation, maintenance and monitoring of compliance with the policy.

The GPO is responsible for conducting a annual review to check firstly that the policy remains suitable for the business and secondly to review policy compliance. This review supports the Group } Œ [• v v µ o]• o } • µ Œ]v šZ Œ ‰ } Œ š v }µvš• Œ P Œ]v P šZ control environment. The GPO is responsible for recommending any changes to the Policy to the relevant Oversight Committee.

The GPO shall ensure appropriate training and resources are in place and that related governance is effective and that this policy is enabling a suitable system of internal control.

The GPO is also accountable for implementing this policy in the business; BU Policy Owners are responsible for ensuring that this policy is implemented in their business areas. The policy is implemented when the:

- Scope of this policy is a fair reflection of current operations and risks the business faces;
- Controls in place meet the minimum control standards in this policy; and
- Controls in place are evidenced as operating effectively.

3.2. Business Unit Policy Owner

The Business Unit Policy Owner (BUPO) is the senior manager within each BU who is responsible for implementing the policy in their business, monitoring compliance and providing demonstrable evidence to the GPO.

The BUPO is responsible for monitoring that this policy is, and remains, embedded by seeking reasonable assurance that relevant risks have been identified and assessed, and that the relevant controls are designed and operating effectively. Changes to this policy can be proposed by the BUPO to the GPO either as part of the annual review process or outside of this, for example, in the event of a major change.

3.3. Employees

All employees of Group Companies are required to comply with this policy to the extent to which it has been adopted by the Group Company in which they are operating (including any local principle or procedure developed in support of the policy).

4. Governanc

4.1. Group Board

The Countrywide Group Board has ultimate accountability for setting and approving the Group's overall governance arrangements. The Board has delegated responsibility for the approval of certain Group Policies to certain committees of the Board and its Executive Committee.

4.2. Executive Committee

The Executive Committee has responsibility for overseeing the design, implementation and maintenance of the Group Policies, and for obtaining assurance that the risk and governance framework is effective. The Executive Committee is supported in discharging its responsibilities via the provision of management information and reporting from the GPO.

4.3. Management Oversight

The BU Managing Directors have identified relevant management committees to oversee compliance with the policy in their businesses. Examples of information the committee will consider (to support the monitoring of compliance with the Policy) include:

- Compliance with policy minimum control standards and any breaches thereof during the period;
- The implications of key corporate projects or new products;
- Reports of incidents, significant external events or new/emerging risks; and
- The status, effectiveness and timeliness of any corrective action plans.

These committees should consider all policy issues referred to them. Any material non-compliance with this policy should be reported to the GPO as soon as is practical by the BUPO. Matters for escalation could include, for example, a material loss arises, a control isn't meeting the CS or a breach of regulatory or legal standards is identified. BU committees are supported in discharging their responsibilities via the provision of management information and reporting from the BUPO.

4.4. Group Risk and Audit

The Group Risk and Audit roles include:

- Supporting the Board and Executive Committees by providing assurance on the design, implementation and maintenance of an effective governance framework, including a system of internal control covering operational, financial, compliance and risk management across the Group
- Supporting the Board and Executive Committees by providing assurance that any areas of significant exposure and/or risk, taking account of all relevant issues including financial considerations, are being managed effectively

- Provision of consolidated, timely and appropriate reporting and escalation of all significant control and risk issues to the appropriate Board / Executive Committee via the Group Policy Owner.

5. Version Control

Version	Approved By	Date
1.0	Group Executive Committee	16 December 2016
1.0	Enterprise Risk Director Annual Review	18 April 2018
2.0	Enterprise Risk Director amended for Criminal Finances Ac	10 September 2018
2.1	Enterprise Risk Director Annual Review	10 August 2019
2.1	GRCC Approval	04 September 2019
2.1	GRCC Approval (following review by Group Financial Contr	July 2020