OPERATIONAL RISK POLICY

SUMMARY FOR THIRD PARTY SUPPLIERS

RATIONALE

Group Policy Rationale

The Operational Risk Policy is designed to ensure that we protect our customers, their money, their data and our colleagues and keep the Group safe by effectively mitigating risks and operational losses through a well-controlled environment.

This Policy defines Lloyds Banking Group's expectations for third party suppliers in managing their operational risks and related events or incidents. We define Operational Risk Management as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events, which can lead to adverse customer impact, reputational damage or financial loss".

Operational Risk is present in all business activities including those carried out by third party suppliers.

SCOPE

This third party version of the Policy applies to suppliers where it has been identified that the Group Policy applies to the provision of their goods and or services.

MANDATORY REQUIREMENTS – GENERAL

KEY DEFINITIONS

- A Risk is a possibility of an event occurring that will have an impact on the achievement of business objectives. An impact is a deviation from the expected in a positive or negative manner.
- A Control is activity undertaken that reduces the probability or impact of a risk occurring.
- An Event is an incident, where operational controls either did not exist or did not operate as intended, and which has resulted in, or could have resulted in, a direct or indirect financial impact (e.g. financial loss, remediation costs, loss of income etc.) and / or a non-financial impact (e.g. customer impact, regulatory breach, reputational damage, etc.).

Third Party Suppliers requirements:

Risk Identification, Assessment and Measurement

- Identify all material operational risks inherent (as defined above) in the businesses' products, activities, people, processes and systems that could impact on the service, customers or reputation of Lloyds Banking Group.
- Assess the potential size of exposure with regards to impacts on customers, financial position or reputation, to the identified risks.
- Identify those exposures where the controls do not mitigate the risk to a level acceptable to the third party supplier's management (i.e. the risk is outside of management's risk appetite and/or the Service Level Agreement(s) in place).
- Take action to bring risks within the supplier's appetite. (This should at least

align to the Service Level Agreement(s) in place).

- Ensure risk records are regularly reviewed and maintained to provide an accurate and up to date view.

Control

- Establish and maintain an effective and efficient control environment to ensure agreed service levels are met and to protect Lloyds Banking Group's customers, reputation, finances and management time & resources.
- Assess design and operating effectiveness of all Key Controls by conducting suitable periodic control assessments / tests (on at least an annual basis) to monitor their ongoing effectiveness.
- Take prompt action where weaknesses and/or gaps are identified in the controls, to optimise the control environment in a cost effective manner.

Events

- Notify the Group as soon as it is reasonably practical of any events as defined above or incidents actually or potentially impacting on the service, customers or reputation of Lloyds Banking Group. This will enable Lloyds Banking Group to assess the size of the issue, escalate appropriately and take any mitigating or remedial actions of its own in a timely manner. Details of the event escalation process will be agreed on a case by case basis in the contract and / or Service Level Agreement.
- Put in place processes to identify & understand Operational Risk Events, including the undertaking of root cause analysis.
- Retain responsibility for management of all Events or incidents.
- Take action to mitigate against future occurrences.

Monitor and Report

- Establish a clear governance structure for the reporting & escalation of operational risk within the Supplier and to Lloyds Banking Group.
- Use management information and indicators to monitor changes in risk exposures and provide early warnings of control weaknesses.
- Reporting and escalation of Events and other Management Information from the supplier to Lloyds Banking Group should normally be carried out via the Supplier Relationship Manager contact within Lloyds Banking Group.

KEY CONTROLS		
Control Title	**Control Description**	**Frequency**
Risks are appropriately identified and managed.	To ensure a good understanding of all the risks a Risk Assessment is undertaken by the Supplier	Annually
Controls Framework in place to sufficiently mitigate the risks identified through the risk assessment.	The Supplier on an ongoing basis develops and implements control activities that mitigate material risks. All controls are assessed /tested (on at least an annual basis) to monitor their ongoing effectiveness.	Annually
Events are reported to Lloyds	The agreed event escalation process	As per

Banking Group on timely basis.	for reporting any relevant Events to Lloyds Banking Group is understood and followed for all events. All events are reported within agreed timescales. (Thresholds for Events required to be reported are agreed with each supplier).	contract
MI regarding Risks and Controls is reported to Lloyds Banking Group within agreed timescales.	Risk and Control management information (MI) is provided to Lloyds Banking Group as specified in the Service Level Agreement and / or contract.	As per contract

MANDATORY REQUIREMENTS – NON-COMPLIANCE

Any material differences between the requirements set out above and the supplier's own controls should be raised by the Supplier with Lloyds Banking Group's Supplier Manager.

The Supplier Manager will then discuss the non compliance with the Accountable Executive for the relationship and local Risk team to agree way forward.

Version Number	Effective Date
6.0	December 2021