OPERATIONAL RISK POLICY

SUMMARY FOR THIRD PARTY SUPPLIERS

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

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”.

The objective is to:

- Ensure governance and accountabilities are in place to demonstrate effective operational risk management.

Customer Impact
The Group’s vision is to be the best bank for customers. The Operational Risk Policy supports this vision and the aim of providing investors with strong, stable and sustainable returns by:

- Protecting customers, keeping the Group safe and efficient, mitigating operational losses through a well controlled business and supporting sustainable growth;
- Supporting the delivery of Group strategy in terms of regulatory expectations and managing the associated risks and objectives within risk appetite.

SCOPE
Activities
The scope of this Policy covers processes conducted by an external party (“the Supplier”) in the course of supplying services for or on behalf of Lloyds Banking Group, or acting on the Group’s behalf (the “Supplier”).

In jurisdictions where the local legislative and regulatory requirements exceed the requirements set out in this document, the Supplier must comply with such higher standards.

KEY DEFINITIONS
- A Risk is a possibility of an event occurring that will have an impact on the achievement of business objectives
- A Control is a process designed to provide reasonable assurance that undesirable events will not occur or will be detected promptly should they occur. Undesirable events include but are not limited to loss or damage to assets (including money), breaches of laws or regulations, loss or degradation in service provision, etc.
OPERATIONAL RISK POLICY

- 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.).

MANDATORY REQUIREMENTS – GENERAL

Third Party Suppliers are required to:

Risk Assessment
- 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.
- Use management information and metrics to monitor changes in risk exposures and provide early warnings of control weaknesses.

Control Activities
- 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 the effective design and operation of all Key Controls (not just those listed below); conducting suitable periodic control tests 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.
REPORTING & ESCALATION

- Establish a clear governance structure for the reporting & escalation of operational risk within the Supplier.
- 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

The following controls must be implemented by the Supplier:

- The agreed Event escalation process for reporting any relevant Events to Lloyds Banking Group is understood and followed for all events. All events are reported 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.

MANDATORY REQUIREMENTS – NON-COMPLIANCE

If a Supplier identifies any breach of the above requirements it must be reported to the Lloyds Banking Group Supplier Relationship Manager or usual business contact as soon as possible after identification.

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Effective Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>August 2014</td>
</tr>
<tr>
<td>2.0</td>
<td>August 2015</td>
</tr>
</tbody>
</table>

**Next Planned Revision:** August 2016