GROUP RESILIENCE & CONTINUITY POLICY SUMMARY FOR THIRD PARTY SUPPLIERS

LLOYDS BANKING GROUP	**GROUP RESILIENCE & CONTINUITY POLICY (INCLUDING INCIDENT MANAGEMENT)** **SUMMARY FOR THIRD PARTY SUPPLIERS**

RATIONALE

This Policy has been designed to assist in managing the risk of potential interruptions from a range of internal and external incidents or threats including environmental and climatic issues, terrorism, economic instabilities, pandemic and operational incidents and to minimise the impact on customers, colleagues and the banking system. The overall risk includes the following risk drivers:

- Failure to effectively identify and classify business processes, their end to end dependencies and to plan, prepare and implement an effective Business Continuity strategy and response framework for significant incidents
- Failure to respond effectively to significant incidents
- Failure to assess the effectiveness of Business Continuity strategy and readiness to respond to significant incidents
- Failure to review and update the response framework for significant incidents
- Failure to maintain an effective and resilient end to end control environment for Critical Business Processes (CBPs)
- Failure to effectively prepare, respond and learn from Building Incidents

In addition this Policy has been designed to support compliance with the following legislation and / or regulations which includes but is not limited to:

- The Financial Conduct Authority (FCA) Handbook and the Prudential Regulation Authority (PRA) Rulebook.
- FCA 'Senior Management Arrangements, Systems and Controls' (SYSC).

The Operational Resilience requirements in this Policy apply to Suppliers providing a service in support of the Group's Critical Business Processes (CBPs) only.

The Group has no appetite for disruptions beyond defined recovery timescales to its material business operations, including impacts to critical customer or colleague services, as a consequence of inadequate or ineffective resiliency and recovery strategies or continuity systems and controls.

Customer Impact

The Group's vision is to be the best bank for customers. The Group Continuity Policy supports this vision by ensuring;

- Appropriate availability of customer products and services and the infrastructure supporting them.
- The Group's requirements for delivering fair outcomes for customers can continue to be met in the event of an incident.
- A proactive and consistent approach to resilience across the Group, through increased knowledge of the CBPs.

GROUP RESILIENCE & CONTINUITY POLICY SUMMARY FOR THIRD PARTY SUPPLIERS

SCOPE

This third party version of the Policy applies to any Supplier that provides goods or services that may be impacted by continuity risks if any of the following apply:

- The service supplied to the Group has to be available in less than 24 hours.
- The service supplied to Group supports a Cat A, B, C CBP
- They provide services either directly or indirectly to Group's customers.

MANDATORY REQUIREMENTS – GENERAL

The Supplier must establish a Resilience & Continuity policy, which is approved in accordance with the Supplier's governance structure, that provides a framework for setting Resilience & Continuity objectives and defines the standards for their implementation and operation. This policy must be reviewed and updated at defined intervals, on a 12 monthly basis as a minimum.

The Supplier must appoint a person, in accordance with the Supplier's governance structure, to be accountable for implementation of this policy, monitoring the Key Controls & Indicators defined below and for confirming to the Group's Supplier Manager that the Supplier's Resilience & Continuity capability meets the Group's requirements.

The Group's approach to Resilience & Continuity is based on four core principles; Operational Resilience, Business Continuity Management, IT Disaster Recovery and Incident Response.

Operational Resilience

Suppliers who are critical to the delivery of the CBPs must meet the following requirements:

- The Supplier must provide sign off on an annual basis to the respective LBG Supplier Manager that the service outlined in the Security Schedule can be met and understand the role they play in the Recovery Time Objective (RTO) of the CBP.

- The Supplier must review their LBG contractual agreements on a 12 monthly basis with Supplier Manager to ensure it remains up to date and fit for purpose.

- The Supplier must provide confirmation that any changes made to the contractual agreements by LBG are understood & embedded within the agreed time scales set by the Supplier Manager.

- The Supplier must comply with any annual assurance undertaken by LBG. Issues identified as a result of the assurance must have appropriate action plans in place with defined dates for action closure.

- The Supplier must define and document the roles and responsibilities of all key person dependencies that underpin the service supporting the LBG CBP.

GROUP RESILIENCE & CONTINUITY POLICY SUMMARY FOR THIRD PARTY SUPPLIERS

- The Supplier must ensure that key staff supporting the CBP service are aware of their roles & responsibilities in relation to the service supporting the LBG CBP on a minimum 12 monthly basis through inductions or training. This may be evidenced by the maintenance of a local induction/training log for key staff.

- The Supplier must identify 4th party Suppliers that are critical to the delivery of the service supporting the LBG CBP and should evidence their ability to meet the CBP Recovery Time Objective (RTO) & Recovery Time Capability (RTC). Any deficiencies/risks must be documented, and actioned where necessary in line with risk appetite.

- The Supplier must identify and document those applications/systems that are critical to the delivery of their service supporting the LBG CBP.

- The Supplier must have appropriate plans in place to manage cyber attacks relating to Confidentiality, Integrity and Availability of the service supporting the LBG CBP.

- The Supplier must ensure that there are no Single Point/s of Failure (SPOF) in relation to key person dependencies as part of the service supporting the LBG CBP.

- The Supplier must ensure that details of key person dependencies, BUs and their continuity arrangements are detailed in the appropriate Business Continuity Plan.
- The Supplier must ensure that, as a minimum, cross site capability is in place for those services provided in support of an LBG CBP.

Business Continuity (BC)

The Supplier must undertake a business continuity impact and risk assessment, at least annually (every 12 months) or in the event of significant operational change. The assessment must identify and classify processes, operational locations, Suppliers/Providers, IT systems, applications and data relative to the impact their interruption or denial would have on the business activities they undertake for or on behalf of the Group and its customers. The assessment should also define minimum recovery requirements including timescales and resources required to continue to provide the contracted goods or services within agreed service levels.

A Continuity strategy and plan to provide operational resilience to reduce the likelihood of interruptions and to mitigate the impact of incidents must be developed and documented. This must evidence as a minimum how the Supplier will manage the denial of people or premises, Technology, data or telecommunications and disruption to their supply chain.

The Supplier must implement and keep up to date documented plans on a 12 monthly basis for managing an incident and any subsequent recovery based on objectives and timescales agreed with the Group. Where a material change to business operations is planned the Supplier must review and update all relevant Continuity documentation and provision ahead of this being implemented. A formal maintenance cycle must be put in place to achieve this requirement.

The capability of the strategy and plans to meet the Group's requirements must be evidenced through an annual (12 monthly) programme of tests and exercises.

Incident Response (IR)

The Supplier must have a defined Incident Response structure to ensure that incidents will be identified, escalated and effectively managed. The structure should allow the Supplier to:

- Decide and communicate the Supplier's strategic response to the incident.
- Manage the operational outcomes of an incident, including implementation of actions to mitigate the impact to the Group.
- Provide the Group with an immediate report on becoming aware of an incident that may impact the Group's customers or the Supplier's ability to continue to provide the contracted goods or services within agreed service levels.

The Incident Response structure must be tested through a relevant scenario based exercise at least annually (every 12 months).

KEY CONTROLS and KEY INDICATORS

The following indicators must be monitored and reported on by the business to evidence operating effectiveness of the mandatory key controls.

Key Control(s)	Key Indicator(s)	Monitoring frequency
Operational Resilience structure in place and tested annually	1. Critical CBP Suppliers must confirm and evidence their capability to meet CBP RTO requirements. This includes confirmation that: a) roles and responsibilities in relation to key person CBP dependencies are defined and documented b) all applications/systems are critical to the delivery of their service have been identified and documented c) no Single Point/s of Failure (SPOF) in relation to key person dependencies have been identified as part of the service d) there is cross site capability for those services provided in support of the LBG CBP 2. Critical CBP Suppliers must provide evidence they have appropriate plans in place to	12 months

	manage cyber attacks relating to Confidentiality, Integrity and Availability of the service supporting the LBG CBP.	
Business Continuity Strategy and Plans are tested annually	1. Undertake the risk assessment annually 2. Develop a strategy and plan 3. Undertake testing and provide proof that changes have been implemented 4. Provide proof that the Supplier's BC capability meets Group requirements 5. Critical CBP suppliers must provide a copy of their Business Continuity Plan or, only in circumstances where they are unable to do so for confidentiality reasons, make this available for inpsection.	12 months
Incident Response structure in place and tested annually	1. Incident Response structure defined and implemented 2. Undertake annual scenario based exercise 3. Number of incidents reported to the Group 4. Provide proof that the Supplier's IR capability meets Group requirements	12 months

MANDATORY REQUIREMENTS – NON-COMPLIANCE
Any material differences between the requirements set out above and the Supplier's own controls should be raised with the Accountable Executive for the relationship by the Supplier Manager and reported to relevant Risk team.

Version Number	Effective Date
1.0	April 2014
2.0	11 September 2014
3.0	13 January 2016
4.0	23 December 2016
5.0	06 June 2017
6.0	24 July 2018
7.0	02 October 2019
Next Planned Revision: July 2020	