GUIDANCE ON CURRENT MINIMUM OPERATIONAL RESILIENCE STANDARDS EXPECTED OF THIRD PARTY SUPPLIERS PROVIDING GOODS AND SERVICES TO LLOYDS BANKING GROUP

NOVEMBER 2020

Control (Process)	Minimum Standard
Scope	These operational resilience standards are designed to assist in managing the risk of potential interruptions from a range of internal and external incidents or threats, to minimise the impact on customers, colleagues and the banking system. The standards detailed below apply to suppliers that provide goods or services that may be impacted by operational resilience risks if any of the following apply; • The service supplied to Lloyds Banking Group supports a Category A or Category B Critical Business Process (CBP) • The service supplied to Lloyds Banking Group has to be available in less than 24 hours • The supplier provides services directly or indirectly to Lloyds Banking Group customers
Contract	The supplier **must be fully aware** of the contractual basis on which it provides services to Lloyds Banking Group (LBG), and in particular the mandated requirements as set out in the Security Schedule (or agreed equivalent contractual terms). The supplier shall, through regular documentation maintenance and testing, confirm to the LBG Supplier Manager that operational changes have been accounted for within Business Continuity documentation and that requirements detailed within the Security Schedule continue to be met.
Business Continuity - Documentation	The supplier must document a Business Continuity Policy and relevant Business Continuity and Disaster Recovery* plans, that reduce the likelihood of interruptions, mitigate the impact from incidents and manage the recovery of services in line with agreed recovery timescales. The supplier will maintain the policy and business continuity plans to ensure they remain relevant and continue to meet the principle aim of ensuring the continued seamless provision of services, with a copy of the documents being provided to Lloyds Banking Group on an annual basis. **Note: the reference to Disaster Recovery plans in this standard is limited to technology used solely by the Supplier in the provision of services to Lloyds Banking Group, and does not include technology used by the Bank or its customers as this is covered under the Technology Policy.*
Business Continuity - Impact Assessment	The supplier must undertake a Business Continuity Impact Assessment on an annual basis, or following significant operational change, to identify the processes that support the provision of services to Lloyds Banking Group, and the impact that a business disruption would have on each of the processes. The business continuity impact assessment should identify the following dependencies for each process: operational locations, IT systems, applications, data, telecommunications and 3rd party suppliers. The assessment should determine the recovery requirements, including timescales and resources required to mitigate the impact and continue the provision of services to Lloyds Banking Group within agreed recovery timescales.

Business Continuity - Plan(s)	The supplier business continuity plans must utilise the Business Continuity Impact Assessment data for processes that support the provision of services to Lloyds Banking Group to develop and document recovery strategies, that address as a minimum how the supplier will manage the following scenarios, and ensure Lloyds Banking Group recovery timescales can be met: • Denial of people (i.e. staff required to undertake/support the service provided to the Bank) • Denial of premises (i.e. where the buildings that the service to the Bank is undertaken cannot be accessed) • Denial of technology, data, or telecommunications (required to perform operations that support the services provided to the Bank) • Disruption to the suppliers' own supply chain The supplier must also ensure that business continuity plans are reviewed and updated annually to reflect any change management activity that impacts business operations, to ensure continuity recovery strategies and timescales can continue to meet Lloyds Banking Group requirements.
Business Continuity - Testing	The capability of the recovery strategies and agreed timescales for processes documented in the business continuity plan, that support the provision of services to Lloyds Banking Group, must be validated through an annual programme of exercising. Exercises should help to identify issues and ensure continuous improvement of the business continuity documentation and recovery capabilities. A post exercise report must be prepared and shared with Lloyds Banking Group to evidence that the exercise included all processes that support the provision of services to Lloyds Banking Group, and the exercise outcomes demonstrated the suppliers capability to meet agreed recovery requirements and timescales. Where the capability to meet agreed recovery requirements and timescales are not demonstrated in the exercising, the supplier will utilise the test outcomes and lessons learned and apply updates to the business continuity policy and busines continuity plan to address these non-compliances. The supplier will provide Lloyds Banking Group with reasonable notice of when Business Continuity tests and exercises are scheduled, in order that the Bank may be present at tests and exercises of the business continuity plans that support the services provided to the Lloyds Banking Group. The supplier must test their Disaster Recovery* plans for critical technology used solely by the Supplier, in the provision of services to Lloyds Banking Group, documenting in post-test reports that the recovery capability meets requirements. **Note: Disaster Recovery testing in this standard is limited to technology used solely by the supplier and does not include technology used by the Bank or its customers as this is covered under the Technology Policy.*
Operational Resilience - Capability	The supplier must provide annual sign-off that they understand the role of the service provided to the Bank in supporting any Bank 'Critical Business Processes' (CBPs). This includes: • Confirmation of the 'Recovery Time Objective' (RTO) of the CBP • Confirmation of the 'Recovery Point Objective' (RPO) of the CBP • Confirmation of the 'Recovery Time Capability' (RTC) of the supplier service

Operational Resilience - Roles & Responsibilities	Roles and responsibilities of all key staff supporting the supplier service to the Bank CBP must be documented and: • Training must be provided at least annually to key staff to ensure these roles and responsibilities are understood. An induction/training log should be maintained to evidence • Single points of failure in relation to key person dependencies should be mitigated • Key person dependencies must have continuity arrangements detailed in the Business Continuity plan
Operational Resilience - Supply Chain	The supplier's own third parties that are critical to the service supporting the Bank CBP must be identified and: • Evidence must be provided they have the required RTC to meet the RTO and RPO of the Bank CBP • Any deficiencies or risks related to these third parties must be documented and timelines agreed with the Bank as to when they will be fully remediated
Operational Resilience - Technology	The applications and systems critical to the delivery of the service supporting the Bank CBP must be identified.
Operational Resilience – Cross-site Capability	Services that support operation of the Bank CBP must have capability to operate from two sites.
Incident Management	The supplier must have an Incident Management procedure that ensures incidents that impact the service being provided to Lloyds Banking Group are identified and effectively managed and include: • A reporting process to immediately alert the Supplier Manager at Lloyds Banking Group of any incident that may impact the ability to continue the provision of services. • A process to manage and remedy the operational outcomes from an incident through the implementation of appropriate actions. • Provision of a detailed incident report to the Bank, which includes an impact summary regarding the service provided to Lloyds Banking Group. • A process to review and implement actions required to prevent a similar incident occurring in the future.