

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

JUNE 2022

Standard	Minimum Standard
<b>Scope</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• The supplier service is utilised by a Lloyds Banking Group Category A or Category B Critical Business Process (CBP) <i>*(1) see below</i></li> <li>• The supplier service is utilised by a Lloyds Banking Group Important Business Service (IBS) <i>*(2) see below and section (Regulatory Policies / Terminology)</i></li> <li>• The service supplied to Lloyds Banking Group (LBG) must be available in less than 24 hours</li> <li>• The supplier provides services directly to LBG customers</li> </ul> <p><i>*(1) Suppliers classified as <b>critical</b> to a CBP by LBG, must comply with all <b>Business Continuity standards</b> and the relevant <b>Operational Resilience Critical Business Process standards</b>.</i></p> <p><i>*(2) Suppliers classified as <b>critical</b> to an IBS by LBG, must comply with all <b>Business Continuity standards</b>, relevant <b>Operational Resilience standards</b> and collaborate with LBG regarding the implementation of <b>IBS standards</b>.</i></p> <p>Suppliers classified against one or more of the following:</p> <ul style="list-style-type: none"> <li>• <b>non-critical</b> supplier / service provided to an LBG CBP or IBS</li> <li>• supplier service must be available in less than 24 hours</li> <li>• supplier provides services directly to LBG customers</li> </ul> <p>must comply with all the <b>Business Continuity standards</b>.</p>

	Supplier service classified by Lloyds Banking Group as follows:						
	Standard	CBP Critical	CBP Non-critical	IBS Critical	IBS Non-critical	Non-CBP / IBS: <24 hr Recovery	Non-CBP/ IBS: direct to LBG customer
<b>Scope (cont.)</b>	BC: Documentation	✓	✓	✓	✓	✓	✓
	BC: Business Continuity Impact Assessment	✓	✓	✓	✓	✓	✓
	BC: Business Continuity Plan(s)	✓	✓	✓	✓	✓	✓
	BC: Business Continuity Testing	✓	✓	✓	✓	✓	✓
	BC: Incident Management	✓	✓	✓	✓	✓	✓
	OR: Capability	✓		✓			
	OR: Roles & Responsibilities	✓		✓			
	OR: Cross-site Capability	✓		✓			
	OR: Technology	✓		✓			
	OR: CBP Supply Chain	✓					
	IBS Testing			✓			
	IBS Supply Chain			✓			
	<b>Regulatory Policies / Terminology</b>	<p>These Operational Resilience 3<sup>rd</sup> Party Minimum Standards incorporate terminology introduced through the Regulators policies published in March 2021. This section provides a brief description of the terminology introduced via the regulatory documentation. Full details of the regulations can be found via the links at the bottom of this section.</p> <p>The Prudential Regulation Authority (PRA) considers “that for firms to be operationally resilient, they should be able to prevent disruption occurring to the extent practicable; adapt systems and processes to continue to provide services and functions in the event of an incident; return to normal running promptly when a disruption is over; and learn and evolve from both incidents and near misses.”</p> <p>The Financial Conduct Authority (FCA) states: “Ensuring the UK financial sector is operationally resilient is important for consumers, firms, and financial markets. It ensures firms and the sector can prevent, adapt, respond to, recover, and learn from operational disruptions”.</p>					

	<p><b>Important Business Services (IBSs):</b></p> <p>An IBS is.  A service that LBG provides that delivers a specific outcome to one or more external customers or clients, and if disrupted or unavailable could</p> <ul style="list-style-type: none"> <li>• pose a risk to the safety and soundness of LBG, undermine policy holder protection, or cause instability in the UK financial system</li> <li>• cause intolerable harm to one or more of LBG’s customers or clients</li> </ul> <p><b>Impact Tolerances:</b></p> <p>An impact tolerance is.  The maximum tolerable level of disruption to an IBS as measured by a length of time in addition to any other relevant metrics. An impact tolerance must be set for each IBS.  Impact tolerances must be set at a point at which any further disruption to the IBS would pose a risk to the firm’s safety and soundness, and in the case of insurers, policyholder protection,</p> <p><b>Severe but plausible disruption scenarios:</b></p> <p>A firm must regularly test their ability to remain within impact tolerances in severe but plausible disruption scenarios. Testing against severe but plausible operational disruption scenarios enables firms to identify vulnerabilities and take mitigating action.  The types of scenario testing undertaken may include paper-based assessments, simulations, or live-systems testing.</p> <p><a href="#">PRA: SS1/21 Operational resilience: Impact tolerances for important business services</a>  <a href="#">PRA: SS2/21 Outsourcing and third-party risk management</a>  <a href="#">FCA PS21-3 Operational Resilience</a></p>
<p><b>Contract</b></p>	<p>The supplier <b>must be fully aware</b> of the contractual basis on which it provides services to LBG, and the mandated requirements as set out in the Security &amp; Resilience 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 &amp; Resilience Schedule continue to be met.</p>
<p>Business Continuity:  <b>Documentation</b></p>	<p>The supplier must document a Business Continuity Policy and relevant Business Continuity and Disaster Recovery* plans, which reduce the likelihood of interruptions, mitigate the impact from incidents and manage the recovery of services in line with agreed recovery timescales.</p> <p>The supplier will maintain the policy and business continuity documentation 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 LBG on an annual basis.</p> <p><i>*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 LBG and does not include technology used by the Bank or its customers as this is covered under the Technology Policy.</i></p>

<p>Business Continuity:</p> <p><b>Business Continuity Impact Assessment</b></p>	<p>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 LBG, and the impact that a business disruption would have on each of the processes.</p> <p>The Business Continuity Impact Assessment should identify the following dependencies (resources) for each process:</p> <ul style="list-style-type: none"> <li>• Operational locations</li> <li>• IT systems, applications</li> <li>• Data</li> <li>• Telecommunications</li> <li>• Key staff resource</li> <li>• Third party suppliers</li> </ul> <p>The assessment should determine the recovery requirements, including timescales and resources required to mitigate the impact and continue the provision of services to LBG within agreed recovery timescales.</p> <p><i>*Nb; BCIA is equivalent to the industry term Business Impact Analysis (BIA)</i></p>
<p>Business Continuity:</p> <p><b>Business Continuity Plan(s)</b></p>	<p>The supplier business continuity plans should utilise the Business Continuity Impact Assessment data for processes that support the provision of services to LBG, to develop and document response and recovery strategies that address as a minimum how the supplier will manage the following denials, and ensure LBG recovery timescales can be met:</p> <ul style="list-style-type: none"> <li>• Denial of people (i.e., staff required to undertake/support the service provided to the Bank)</li> <li>• Denial of premises (i.e., where the buildings that the service to the Bank is undertaken cannot be accessed)</li> <li>• Denial of technology, data, or telecommunications (required to perform operations that support the services provided to the Bank)</li> <li>• Disruption to the suppliers' own supply chain</li> </ul> <p>The supplier must review their business continuity plan(s) and recovery strategies regularly and where appropriate, update to mitigate risks from emerging threats (e.g., climate change) to ensure the continued provision of services to LBG within agreed recovery timescales.</p> <p>The supplier must ensure that business continuity plans are reviewed and updated annually to reflect any change management activity that impacts business operations, to ensure continuity response and recovery strategies and timescales can continue to meet LBG requirements.</p>
<p>Business Continuity:</p> <p><b>Business Continuity Testing</b></p>	<p>The capability of the supplier recovery strategies and agreed recovery timescales for processes documented in the business continuity plan, which support the provision of services to LBG, need to be validated through an annual programme of tests &amp; exercises.</p> <p>Testing &amp; exercising should help to identify issues and ensure continuous improvement of the business continuity documentation and recovery capabilities.</p> <p>A post-test &amp; exercise report must be prepared and shared with LBG to evidence that the test / exercise included all processes that support the provision of services to LBG, and the test / exercise outcomes demonstrated the supplier's capability to meet agreed recovery requirements and timescales.</p> <p>Where the capability to meet agreed recovery requirements and timescales are not demonstrated in the testing or exercising, the supplier will utilise the test outcomes and lessons learned and apply updates to the business continuity</p>

<p>Business Continuity:</p> <p><b>Business Continuity Testing (cont.)</b></p>	<p>documentation, as appropriate, to address these vulnerabilities and non-compliances.</p> <p>The supplier will provide LBG 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 LBG.</p> <p>The supplier must test their Disaster Recovery*(see below) plans for critical technology used solely by the Supplier, in the provision of services to LBG, documenting in post-test reports that the recovery capability meets requirements.</p> <p><i>*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.</i></p>
<p>Business Continuity:</p> <p>–</p> <p><b>Incident Management</b></p>	<p>The supplier must have an Incident Management procedure that ensures incidents that impact the service being provided to LBG are identified and effectively managed and include:</p> <ul style="list-style-type: none"> <li>• A reporting process to immediately alert the Supplier Manager at LBG of any incident that may impact the ability to continue the provision of services.</li> <li>• A process to manage and remedy the operational outcomes from an incident through the implementation of appropriate actions.</li> <li>• Provision of a detailed incident report to the Bank, which includes an impact summary regarding the service provided to LBG.</li> </ul> <p>A process to review and implement actions required to prevent a similar incident occurring in the future</p>
<p>Operational Resilience:</p> <p><b>CBP &amp; IBS Capability</b></p>	<p>Where a supplier service is critical to an LBG CBP or IBS, the supplier must provide annual written sign-off to the LBG Supply Manager, that they understand the role of the service provided to the Bank and utilised by either a CBP or IBSs.</p> <p>Sign off to include:</p> <ul style="list-style-type: none"> <li>• Confirmation of the 'Recovery Time Objective' (RTO) of the CBP or IBS that utilises the supplier service</li> <li>• Confirmation of the 'Recovery Point Objective' (RPO) of the CBP or IBS that utilises the supplier service</li> <li>• Confirmation of the 'Recovery Time Capability' (RTC) of the supplier service that is utilised by a CBP or IBS</li> <li>• Confirmation that identified issues preventing Operational Resilience Minimum Standards being met by the supplier, are documented with remediation actions raised and shared with LBG</li> </ul>
<p>Operational Resilience:</p> <p><b>CBP &amp; IBS Roles &amp; Responsibilities</b></p>	<p>Where the supplier service is critical to an LBG CBP or IBS, roles and responsibilities of all key staff supporting the supplier service to CBPs, or IBSs must be documented and:</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• Single points of failure in relation to key person dependencies should be mitigated</li> <li>• Key person dependencies must be operationally resilient, with arrangements and succession planning detailed in the relevant Business Continuity documentation</li> </ul>

	<ul style="list-style-type: none"> <li>• Capability established to monitor absence and attrition rates of key staff supporting the service provided to Lloyds Banking Group.</li> </ul>
<p>Operational Resilience:</p> <p><b>CBP &amp; IBS</b></p> <p><b>Cross-site Capability</b></p>	<p>Where the supplier service is critical to an LBG CBP or IBS, the supplier must have the capability to operate the end-to-end service from two sites.</p> <p>Where agreed with LBG, the secondary location may include suitable working from home arrangements.</p>
<p>Operational Resilience:</p> <p><b>CBP &amp; IBS</b></p> <p><b>Technology</b></p>	<p>Where the supplier service is critical to an LBG CBP or IBS, the applications, and systems critical to the delivery of the service utilised by an LBG CBP or IBS must be identified.</p> <p><i>Note: Operational Resilience requirements for third parties that supply technology to LBG must meet the standards detailed within the LBG third-party Technology policy.</i></p>
<p>Operational Resilience:</p> <p><b>CBP</b></p> <p><b>Supply Chain</b></p>	<p>Where the supplier service is critical to a LBG CBP, the supplier’s own third parties (also referred to as fourth parties), that are critical to the service utilised by the Bank CBP must be identified and on an annual basis:</p> <ul style="list-style-type: none"> <li>• Evidence must be provided to the supplier that the supplier’s own third parties have the required Recovery Time Capability (RTC) to meet the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) of the CBP utilising the service.</li> <li>• Any deficiencies or risks related to these third parties of the LBG supplier must be documented, and shared with LBG, with timelines agreed with the Bank as to when they will be fully remediated.</li> </ul>
<p><b>IBS</b></p> <p><b>Testing</b></p>	<p>Where the supplier service is critical to a LBG IBS, the supplier may be asked to collaborate during severe but plausible scenario exercises, delivered by LBG, through either participating or sharing information regarding their response and recovery capability, to recover the service within the defined impact tolerance.</p>
<p><b>IBS</b></p> <p><b>Supply Chain</b></p>	<p>Where the supplier service is critical to a LBG IBS, the supplier’s own third parties (also referred to as fourth parties), that are critical to the service utilised by the Bank IBS, must be identified and on an annual basis:</p> <ul style="list-style-type: none"> <li>• Evidence must be provided to the supplier that the supplier’s own third parties have the required Recovery Time Capability (RTC) to meet the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) of the IBS utilising the service.</li> <li>• Any deficiencies or risks related to these third parties of the LBG supplier, must be documented, and shared with LBG, with timelines agreed with the Bank as to when they will be fully remediated.</li> </ul> <p>The supplier may be asked by LBG that their own third parties collaborate during severe but plausible scenario exercises, delivered by LBG, through either participating or sharing information regarding the supplier’s third-parties response and recovery capability, to recover the service within the defined impact tolerance.</p>