

External Supplier Control Obligations

Recovery Planning

1. Definitions:

“Disruption Event”	A register of Incident impacts, agnostic of cause, that Suppliers have chosen to mitigate through the implementation of recovery and resilience planning and capabilities.
“Incident”	Means a disruptive event that can be managed as part of day-to-day operations, through the invocation of recovery plans.
“Recovery Plan”	Recovery Plans are documents which detail the steps and actions to be taken to restore a service back to operational status. These may be called Business Continuity Plan or similar terms.
“Recovery Planning”	The process or planning for the recovery of business services, business process and the underlying dependencies.
“Recovery Time Objective”	Means the time between an unexpected failure or interruption of services and the resumption of operations.
“Resilience Category”	Resilience Category is a rating used by Barclays to apply resilience requirements to a service. The Resilience Category drives Recovery Time Objective (RTO), Recovery Point Objective (RPO) and validation frequency requirement.

2. Resilience Criticality Matrix:

Supplier’s services are assigned to a specific Resilience Category (0-4) by Barclays which reflects the impact to Barclays that a disruption of the service may cause. A higher Resilience Category (i.e. lower number) will require a higher standard of resilience or recovery commensurate with the importance of the service. Supplier shall ensure that its services achieve the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) specified below for the applicable Resilience Category stipulated by Barclays for the contracted services. The following table specifies which Supplier Controls are applicable based on the defined Resilience Category, and the details of those Controls are set out at section 3 (*Control*) below.

Risk Impact Assessment	Exceptional Impact	High Impact	Moderate Impact	Low Impact	Insignificant Impact
Resilience Category	0	1	2	3	4
RTO Target	Up to 1 hour	Up to 4 hours	Up to 12 hours	up to 24 hours	No planned recovery
RPO Target	Up to 5 minutes	Up to 15 mins	Up to 30 mins	Up to 24 hours	No planned recovery

Technology Testing Frequency	Resilience Category 0	Resilience Category 1	Resilience Category 2	Resilience Category 3	Resilience Category 4
System Recovery Plan Validation	Min twice yearly	Min twice yearly	Min every 12 months	Min every 24 months	No planned recovery
Data Recovery Plan Validation	Annual validation of plan in Production-like environment	Annual validation via desktop walkthrough	Optional	Optional	No planned recovery
Platform and Application Rebuild Plan Validation	Annual validation via desktop walkthrough	Annual validation via desktop walkthrough	Optional	Optional	No planned recovery

Supplier Controls Applicability	Resilience Category 0	Resilience Category 1	Resilience Category 2	Resilience Category 3	Resilience Category 4
1. Dependency Mapping Requirement for inclusion with Recovery Planning	✓	✓	✓	✓	○
2. Disruptive Events for Recovery Planning Requirement	✓	✓	✓	✓	○
3. Recovery Planning & Validation Requirement	✓	✓	✓	✓	○
4. Integrated Testing Requirement	✓	✓	○	○	○
5. System Recovery Plans & Validation Requirement	✓	✓	✓	✓	○
6. Data Recovery Plans & Validation Requirement	✓	✓	○	○	○
7. Data Centre Diversity & Cloud Service Provider Requirement	✓	✓	✓	✓	○
8. Platform and Application Rebuild Plans & Validation Requirement	✓	✓	○	○	○

✓ = Required	○ = Optional
--------------	--------------

If any issues are identified during review or failure to meet requirements during testing of controls, the Supplier must notify Barclays promptly (typically within 10 days) and remediate issues by an agreed date.

3. Controls:

Supplier must have a Structured Approach to Resilience (Business Continuity and Disaster Recovery) that is supported by a Policy and Standards document that govern Operational and Technical resilience requirements in line with industry best practices and regulatory requirements as applicable. The Structured Approach to Resilience must be overseen by Senior Management and reviewed and tested for effectiveness on an annual basis.

Control Title	Control Description	Why this is important
<p>1. Dependency Mapping Requirement for inclusion within Recovery Planning</p>	<p>Supplier must define and document dependencies which are critical to delivering the service to Barclays. These dependences must be maintained and reviewed every 12 months or when material change occurs.</p> <p>Dependences to consider include:</p> <ul style="list-style-type: none"> ▪ Technology and data (internal and Sub-contractor provided). ▪ Material Subcontractor(s) (who could have a material impact on the performance and provision of the service to Barclays). ▪ Workforce (Loss of people; consider no work area recovery strategy or working from home capability). 	<p>Service providers need to understand dependencies for providing their service to Barclays. Any dependencies will form part of their Business Recovery Plan to ensure these are considered in order to mitigate the impact of incidents and prevent the unavailability of the service to Barclays.</p>
<p>2. Disruptive Events for Recovery Planning Requirement</p>	<p>Supplier must define the disruptive events in scope for recovery planning, and the level of planning required to ensure the services can be delivered within the agreed service levels and the corresponding Recovery Time Objectives. Supplier must ensure such Disruption Events remain reflective of the current risk/threat landscape, are assessed for severity and plausibility, and supported by industry and intelligence insights.</p> <p>As a minimum the Supplier must include the following Disruption Events in the scope of its planning.</p> <ul style="list-style-type: none"> ▪ Loss of building(s) across multiple locations impacting delivery of services to Barclays. (Buildings and associated infrastructure are unavailable). ▪ Loss of data scenario, including cyber events and the potential impact on the delivery of services to Barclays. ▪ Loss of workforce resources which would impact delivery of agreed service levels (i.e. pandemic event, geopolitical event, critical national infrastructure failure, etc.). ▪ Loss of technology services (i.e. loss of data centres or Cloud Service Provider Region). 	<p>Barclays has a commercial (and risk-driven) requirement to avoid and/or be able to recover in a timely manner from significant Disruption Events i.e. to be suitably resilient. Barclays must be assured and must be able to assure its stakeholders that if disruptions occur, the service is designed to minimise their impact (whether customer, financial and/or reputational impact).</p>

Control Title	Control Description	Why this is important
	<ul style="list-style-type: none"> ▪ Loss of Material Subcontractor (Services or Supplies). <p>Disruption Events must be reviewed annually, and on a continuous basis, to inform planning and testing and demonstrate how this evolves over time.</p>	
<p>3. Recovery Planning & Validation Requirement</p>	<p>Supplier must maintain Recovery Plans for its agreed Disruption Events.</p> <p>Recovery Plans should document the detailed recovery steps and Supplier response which is possible to mitigate the impact and/or defer the unavailability of services provided to Barclays.</p> <p>As a minimum this should consider:</p> <ul style="list-style-type: none"> ▪ Possible workarounds ▪ Decision Protocols ▪ Communication and business prioritisation to resume/maintain a minimum viable service ▪ Dependencies <p>Recovery Plans must be tested and validated every 12 months, or when a material change occurs, to demonstrate that agreed service levels can be delivered and that the services meet the Resilience Category requirements stipulated by Barclays.</p> <p>If any plan fails to achieve the agreed service levels or applicable Resilience Category requirements, Supplier must promptly notify Barclays (typically within 10 days) and provide detailed remediation plans (including actions to be undertaken and corresponding completion dates).</p>	<p>Testing and validation is completed to assure Barclays that the service design and plan works as intended and includes all dependencies and demonstrates that the agreed service levels can be delivered and that the services meets the resilience requirements stipulated by Barclays.</p>
<p>4. Integrated Testing Requirement</p>	<p>To ensure that interdependencies between Barclays and Supplier Services are understood in relation to service recovery, the Supplier at the request of Barclays and on a mutually agreed date, must participate in an integrated test to validate the collective resilience/continuity of both Supplier and Barclays.</p>	<p>Joint exercises help ensure that there are adequate Recovery Planning protocols in place, with effective communication strategies being adopted, and that both Supplier and Barclays are taking a co-ordinated response to managing business disruption and minimising the impact on Barclays' customers and the wider financial system.</p>

Control Title	Control Description	Why this is important
	<p>Barclays will not make this request more than once every 2 years unless previous integrated tests have highlighted material shortfalls or there has been an incident causing disruption of services.</p>	
<p>5. System Recovery Plans & Validation Requirement</p>	<p>Supplier must have a System Recovery Plan that details actions required to recover systems back to operational state following a disruption. The plans must be tested and validated to demonstrate (with evidence) that the system can be recovered within the defined Recovery Time Objective and Recovery Point Objective as required by the defined Resilience Category.</p> <p>For systems designed in an active/passive configuration, the passive environment must be activated and used as a BAU production environment for a duration long enough to prove capability and full integration functionality.</p> <p>For services designed as active/active, validation should prove the continued operation under the loss of a node, instance, or Availability Zone (for Cloud hosted) of the system (minimum 60 minutes).</p> <p>Validation frequency requirements are defined by the Resilience Category for the system. See the above Resilience Criticality Matrix</p>	<p>Absent or inadequate System Recovery Plans may lead to unacceptable loss of technology service to Barclays or its clients following an Incident. Keeping resilience documentation updated and practiced ensures that recovery plans remain aligned to business needs.</p>
<p>6. Data Recovery Plans & Validation Requirement</p>	<p>Supplier must have Data Recovery Plan(s) for each technology system required to support the delivery of services to Barclays. Plan(s) must be reviewed for accuracy at least once every 12months, or when a material change occurs, and should consider as a minimum the following:</p> <ul style="list-style-type: none"> ▪ Data sources and flow (upstream and downstream) ▪ Backup and replication sources ▪ Data synchronisation requirements post restore <p>Supplier must test and validate the Data Recovery Plan(s) for each technology system required to support the delivery of services to Barclays and prove (with evidence) the recovery process can recover data to expected operational state and within required Recovery Point Objective.</p>	<p>Loss of data is one of the biggest threats Barclays faces, and this can come by way of malicious acts or system failure. Having a plan for this scenario is critical and helps identify and understand sources of data and dependencies.</p>

Control Title	Control Description	Why this is important
<p>7. Data Centre Diversity & Cloud Service Provider Requirement</p>	<p>Supplier must ensure that each technology system required to support the delivery of services to Barclays is resilient across data centres and far apart enough geographically, to reduce the risk of data centres being impacted simultaneously by a single event.</p> <p>Where the technology system is hosted on a Cloud Service Provider, the system should be available across different Availability Zones to mitigate against an AZ outage. Critical systems are required to demonstrate the ability to recover from a Cloud Service Provider Region failure.</p>	<p>Technology systems should be deployed across multiple data centres to protect against a Data Centre outage. This extends to systems hosted on Cloud Service Provider - Region failure.</p>
<p>8. Platform and Application Rebuild Plans Requirement</p>	<p>Supplier must maintain a Platform and Application Rebuild Plan for each technology system required to support the delivery of services to Barclays and be subject to review, approval and testing at least once every 12 months, or when a material change occurs.</p> <p>These plans are for situations where traditional recovery/restore options can't be used and the system needs to be rebuilt from 'bare metal'.</p> <p>Plans should consider:</p> <ul style="list-style-type: none"> ▪ Operating system/infrastructure software ▪ Application deployment and configuration ▪ Security controls/configuration ▪ System ecosystem dependencies and re-integration ▪ Data Requirements (Data Recovery Plan) ▪ Tooling dependencies to execute recovery plans 	<p>It is critical that technology services and support arrangements have appropriate recovery plans for a Cyber / Data Integrity event.</p>