BARCLAYS

# External Supplier Control Obligations

## Recovery Planning

Version 11.0 Dated October 2021

# 1. Definitions:

| | |
|---|---|
| **"Crisis"** | means a disruptive or reputational event requiring a response which is beyond the normal BAU structure and/or resources and requires executive intervention for decision making and coordination. |
| **"Incident"** | means a disruptive event that can be managed as part of day-to-day operations, through the invocation of recovery plans. |
| **"Recovery Planning"** | The process or planning for the recovery of business services, business process and the underlying dependencies |
| **"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 |
| **"Recovery Time Objective"** | means the time between an unexpected failure or interruption of services and the resumption of operations. |

# 2. Controls:

| Control Title | Control Description | Why this is important |
|---|---|---|
| 1. Disruptive Events for Recovery Planning requirements | Barclays shall stipulate the Resilience Category for the contracted services.<br><br>The Supplier must define the disruptive events in scope for 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.<br><br>Disruption Event categories should consider as a minimum:<br><br>▪ Loss of building(s) across multiple locations unable to support business operations;<br>▪ Loss of data scenario, including cyber events and the potential impact on the delivery of services to Barclays. Loss of colleague resources which would impact delivery of agreed service levels;<br>▪ Unavailability of services to Barclays due to potential cyber/non cyber events, and the potential impact on the delivery of service to Barclays;<br>▪ Single and concurrent recovery of technology services (i.e. loss of data centre)<br><br>Disruption events must be reviewed annually, and on a continuous basis, to inform planning and testing and demonstrate how this evolves over time. | Barclays has a commercial (and risk-driven) requirement to avoid and/or be able to recover in a timely manner from significant Disruptive 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). |

| Control Title | Control Description | Why this is important |
|---|---|---|
| | Supplier must be able to demonstrate that a variety of severity factors have been considered, tested and validated. | |
| 2. Dependency Mapping requirements for inclusion within Recovery Planning | Supplier must define and document dependencies which are critical to delivering the service to Barclays to ensure these are equally resilient for Supplier. These dependences must be maintained and reviewed every 12 months.<br><br>Dependences to consider include:<br><br>▪ Loss of all technology and data<br>▪ Unavailability of services from Material Subcontractor(s) (those that are critical to providing the service to Barclays)<br>▪ Loss of workforce (loss of buildings or/and Loss of people; consider no work area recovery strategy or working from home capability)<br><br>These must be tested and validated through the Business Recovery Plan, to demonstrate that the services meet the Resilience Category requirement stipulated by Barclays to ensure these are equally resilient and meet the required service levels. | 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. |
| 3. Validation of Recovery Planning Requirements | Supplier must maintain Business Recovery Plans for their agreed Disruption Events.<br><br>Business Recovery Plans should document the detailed recovery steps and Supplier response which is possible to mitigate the impact and/or defer the unavailability of the service provided to Barclays.<br><br>As a minimum this should consider:<br><br>▪ Possible workarounds<br>▪ Decision Protocols<br>▪ Communication and business prioritisation to resume/maintain a minimum viable service<br>▪ Dependencies | 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. |

| Control Title | Control Description | Why this is important |
|---|---|---|
| | Recovery Plans must be tested and validated every 12 months to demonstrate that agreed service levels can be delivered and that the services meet the Resilience Category requirements stipulated by Barclays.<br><br>If any plan fails to achieve the agreed service levels or applicable Resilience Category requirements, Supplier must promptly notify Barclays and provide detailed remediation plans (including actions to be undertaken and corresponding completion dates). | |
| 4. Integrated Testing | Supplier at the request of Barclays, must participate in an integrated test to validate the collective resilience/continuity of both Supplier and Barclays.<br><br>Barclays will not make this request more than once every 2 years unless previous integrated tests have highlighted material shortfalls or there are material changes to the services. | 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. |
| 5. Incident/Crisis Management Procedure | Supplier must have a documented Incident and Crisis management procedure which includes the process for escalating Incidents/Crises to Barclays. Incident and Crisis management procedures must be approved after successful testing and validation by Supplier every 12 months.<br><br>The procedure must define the minimum activities and outcomes required for managing and handling the Incident/Crisis through its lifecycle from inception through to closure. Supplier shall nominate:<br><br>(i) an individual as the approver of the procedure, responsible for confirming that it is fit for purpose;<br><br>(ii) a primary contact and a deputy (in case of the primary contact's absence) for each Crisis role; | Supplier needs to be clear on its procedures to handle and manage its services in the event of an Incident or Crisis. Supplier and Barclays must have a shared understanding of the escalation process for Incident and Crisis situations.<br><br>Testing and validation must be completed to ensure that the relevant individual/team has sufficient skills, knowledge and organisation to manage Incidents and Crises as and when they arise. |
| 6. Post Incident/Crisis Reporting | Following a disruption to the service, a Post Incident/Crisis Report must be provided to Barclays within four calendar weeks of the reinstatement of the service to normal operating levels.<br><br>The report must include as a minimum a review of: | Post Incident/Crisis Reporting is required to assure Barclays that issues are identified/remediated, and lessons are learned, in a timely manner. |

| Control Title | Control Description | Why this is important |
|---|---|---|
| | ▪ the root cause of the Incident or Crisis<br>▪ remediation steps completed, and any continuous improvement actions to prevent reoccurrence<br>▪ any impact to Barclays customers known to Supplier | |
| 7. System Recovery Plans | Supplier must have System Recovery Plan(s) (SRP) for each technology system/service required to support the delivery of Barclays Resilience Category 0-3 services, and the corresponding Recovery Time Objectives (RTO) and Recovery Point Objective (RPO). Plan(s) must be reviewed for accuracy at least once every 12 months.<br><br>Note: for Resilience Category 0-1 technology systems/services, that are designed in an active/passive configuration for resilience measures, validation of the SRP requires that the system remains in the recovered environment for an extended period and operate as BAU, to confirm that all elements operate effectively. This in effect is a Production Crossover (PCO) event. | 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. |
| 8. Data Integrity Recovery Plans | Supplier must have Data Integrity and Recovery Plan(s) (DIRP) for each technology system/service required to support the delivery of Barclays Resilience Category 0-1 services. Plan(s) must be reviewed for accuracy at least once every 12months. | Loss of data is one of the biggest threats we face, 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. |
| 9. Data Centre Diversity | Supplier must ensure that each technology system/service required to support the delivery of Barclays Resilience Category 0-3 services is resilient across data centres and far apart enough to reduce the risk of data centres being impacted simultaneously by a single event. | Data Centres should have alternate power sources, network links, etc. and be far apart enough to reduce risk of data centres being impacted simultaneously by a single event. |
| 10. SRP Validation | Supplier must test and validate the System Recovery Plan(s) (SRP) to demonstrate that the technology system/services can be recovered to meet the Resilience Category 0-3 requirements stipulated by Barclays.<br><br>For each technology system/service required to support the delivery of Resilience Category 0-1 services, that are designed in an active/passive configuration for resilience measures, the passive environment must be activated following the documented SRP and used as a BAU production environment, for a duration long enough to prove capability and full integration functionality (Production Crossover). | Third party provided technology systems can impact Barclays customer journeys. Ensuring third parties that support Barclays business operations have adequate resilience plans that are tested is crucial and also a Regulatory mandate for Barclays to apply proper governance in managing our suppliers.<br><br>Production Crossover (PCO) is a method to validate that the passive instance of an active-passive configured system |

| Control Title | Control Description | Why this is important |
|---|---|---|
| | Validation frequency requirements must be supported by the associated Resilience Category i.e.:<br><br>-Resilience Category 0: SRP validation must be performed as a minimum four times per year via PCO.<br>-Resilience Category 1: SRP and PCO validation must be performed as a minimum twice yearly via PCO<br>-Resilience Category 2: SRP validation must be performed as a minimum every 12 months;<br>- Resilience Category 3: SRP validation must be performed as a minimum every 24 months<br><br>If any testing fails to achieve the minimum recovery requirements for the applicable Resilience Category, Supplier must promptly notify Barclays and provide detailed remediation plans (including actions to be undertaken and corresponding completion dates). Supplier must notify Barclays prior to executing PCO. | works as expected and to the capacity that is required in BAU operation. In addition, a PCO also validates that any dependency on upstream or downstream systems continue to function as expected. |
| 11. DIRP Validation | Supplier must test and validate the Data Integrity and Recovery Plan(s) (DIRP) for each technology system/service required to support the delivery of Barclays Resilience Category 0-1 services, to prove the integrity of data during recovery. Validation should be performed at least once every 12 months.<br><br>If any plan fails to achieve the minimum recovery requirements for the applicable Resilience Category, Supplier must promptly notify Barclays and provide detailed remediation plans (including actions to be undertaken and corresponding completion dates). | Data is a critical element that can be adversely impacted in many ways. The documented plan to restore, recover or recreate data must be exercised to confirm it is accurate and viable. |
| 12. Platform and Application Rebuild / Repave plans | To support recovery from Disruption Events such as a cyber exploit, the Supplier must have a Platform and Application Rebuild / Repave Plan for each technology service/system required to support the delivery of Barclays Resilience Category 0-1 services and be subject to review, approval and testing at least once every 12 months.<br><br>If any plan fails to achieve the minimum recovery requirements for the applicable Resilience Category, Supplier must promptly notify Barclays and provide detailed remediation plans (including actions to be undertaken and corresponding completion dates). | Technology services and support arrangements have appropriate recovery plans for a Cyber / Data Integrity event. |

# 3. Resilience Criticality Matrix:

Supplier's services are assigned to a specific Resilience Category (0-4) by Barclays. 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) specified below for the applicable Resilience Category stipulated by Barclays:

| | | ERMF - Risk Impact Assessment | Exceptional Impact | High Impact | Moderate Impact | Low Impact | Insignificant Impact |
|---|---|---|---|---|---|---|---|
| | | Resilience Category | 0 | 1 | 2 | 3 | 4 |
| | | Resilience Type | Continuous | Highly Resilient | Resilient | Recover | Suspend / Backup Only |
| Disruption Event | Application | RTO for Application Recovery (non-data events) | Up to 1 hour | Up to 4 hours | Up to 12 hours | up to 24 hours | No planned recovery |
| | | RPO | Up to 5 minutes | Up to 15 mins | Up to 30 mins | Up to 24 hours | No planned recovery |