BARCLAYS

External Supplier Control Obligations

Resilience

Version 9.0 April 2019

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 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. Service Design Resilience Requirements	Barclays shall stipulate the Resilience Category for the services, and Supplier shall ensure that the services are designed to deliver to the corresponding Recovery Time Objectives (RTO), as set out below.	Barclays has a commercial (and risk-driven) requirement to avoid and/or be able to recover in a timely manner from significant process disruptions 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).
2. Validation of Resilience Requirements	For the purposes of this Control Description, a service "component" comprises of anything that facilitates delivery of that service including but not limited to people, facilities, suppliers, IT applications and infrastructure. Supplier must test and validate the service components every 12 months to demonstrate that the services meets the Resilience Category requirements stipulated by Barclays. If any service component fails to achieve the applicable Resilience Category requirements, Supplier must promptly notify Barclays and provide detailed remediation plans (including actions to be undertaken and corresponding completion dates).	Testing and validation is completed to assure Barclays that the service design works as intended and achieves the resilience requirements stipulated by Barclays.

Control Title	Control Description	Why this is important
3. 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. 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: (i) an individual as the approver of the procedure, responsible for confirming that it is fit for purpose; and (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. Supplier must complete testing and validation to ensure that the relevant individual/team has sufficient skills, knowledge and organisation to manage Incidents and Crises as and when they arise.
4. 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. The report must include as a minimum a review of: • the events surrounding the situation; • how the Incident/Crisis was managed; • analysis of its root cause; • whether it is classed as a 'Risk Event' by Supplier or Barclays (i.e. deemed sufficiently significant that it should be notified/escalated to relevant stakeholders in accordance with the applicable policies known to Supplier); • whether it represents a 'Conduct Risk' (e.g. if Supplier is dealing directly with Barclays' customers); • any Barclays' customer-redress known to Supplier; and • any steps required to prevent reoccurrence of similar Incidents/Crises.	Post Incident/Crisis Reporting is required to assure Barclays that issues are identified/remediated, and lessons are learned, in a timely manner.

3. Resilience Criticality Matrix:

Supplier's services are assigned to a specific Resilience Category (0-3) 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:

Resilience Category	0	1	2	3
Recovery Time Objective (RTO)	0 Sec	< 4 Hours	< 12 Hours	24 Hours