BARCLAYS

External Supplier Control Obligations

Recovery Planning

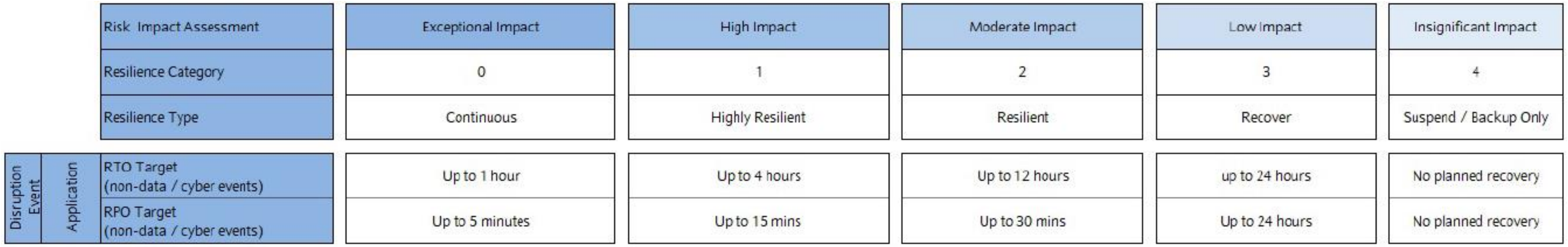
Version 12.0 October 2022

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.
“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.
“Production Crossover”	Production Crossover is a term used for when a technology system is failed over to an alternate environment (DR) and used to run production functions for an extended period of time.
“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 to apply resilience requirements to a service. These include RTO, RPO, validation requirements and frequency.

2. 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) and Recovery Point Objective (RPO) specified below for the applicable Resilience Category stipulated by Barclays for the contracted services:



			Exceptional Impact	High Impact	Moderate Impact	Low Impact	Insignificant Impact
		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 Target (non-data / cyber events)	Up to 1 hour	Up to 4 hours	Up to 12 hours	up to 24 hours	No planned recovery
		RPO Target (non-data / cyber events)	Up to 5 minutes	Up to 15 mins	Up to 30 mins	Up to 24 hours	No planned recovery

3. 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. 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. Disruption Event planning should consider as a minimum: ▪ 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 impacting all technology services). ▪ Loss of material subcontractor (Services or Supplies). Disruption events must be reviewed annually, and on a continuous basis, to inform planning and testing and demonstrate how this evolves over time. Supplier must be able to demonstrate that a variety of severity factors have been considered, tested and validated.	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).
2. Dependency Mapping requirements for inclusion within Recovery Planning	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. Dependences to consider include: ▪ Technology and data (internal and sub-contractor provided). ▪ Material Subcontractor(s) (those that are critical to providing the service to Barclays). ▪ Workforce (Loss of people; consider no work area recovery strategy or working from home capability).	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.

Control Title	Control Description	Why this is important
3. Validation of Recovery Planning Requirements	Supplier must maintain Business Recovery Plans for its agreed Disruption Events. 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 services provided to Barclays. As a minimum this should consider: ▪ Possible workarounds ▪ Decision Protocols ▪ Communication and business prioritisation to resume/maintain a minimum viable service ▪ Dependencies 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. 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).	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.
4. Integrated Testing	Resilience Category 0-1 Supplier at the request of Barclays on a mutually agreed date, must participate in an integrated test to validate the collective resilience/continuity of both Supplier and Barclays. 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.	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.

Control Title	Control Description	Why this is important
5. System Recovery Plans	Supplier must have System Recovery Plan(s) (SRP) for each technology system/service required to support the delivery of services to Barclays, 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.	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.
6. Data Recovery Plans	Resilience Category 0-1 Supplier must have Data Recovery Plan(s) for each technology system/service required to support the delivery of services to Barclays. Plan(s) must be reviewed for accuracy at least once every 12months and should consider as a minimum the following: • Data sources and flow (upstream and downstream) • Backup and replication sources • Data synchronisation requirements post restore	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.
7. Data Centre Diversity	Supplier must ensure that each technology system/service required to support the delivery of services to Barclays is resilient across data centres and far apart enough to reduce the risk of data centres being impacted simultaneously by a single event. Where the technology system is hosted on a Cloud Service Provider, the service should be available across different Availability Zone to mitigate against a AZ outage. ResCat 0-1 services should be resilient across Cloud Regions.	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.
8. System Recovery Plan Validation	Supplier must test and validate the System Recovery Plan(s) to demonstrate that the technology system/services can be recovered and meet the Recovery Time Objective and Recovery Point Objective as defined by the Resilience Criticality Matrix. 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 System Recovery Plan and used as a BAU production environment, for a duration long enough to prove capability and full integration functionality (Production Crossover). For services designed as active/active, validation should prove the continued operation under the loss of one active environment (Reduced processing resource scenario).	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. Production Crossover (PCO) is a method to validate that the passive instance of an active-passive configured system 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.

Control Title	Control Description	Why this is important
	Validation frequency requirements must be supported by the associated Resilience Category i.e.: -Resilience Category 0: SRP validation must be performed as a minimum four times per year via PCO. -Resilience Category 1: SRP and PCO validation must be performed as a minimum twice yearly via PCO. -Resilience Category 2: SRP validation must be performed as a minimum every 12 months. - Resilience Category 3: SRP validation must be performed as a minimum every 24 months. 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).	
9. Data Recovery Plan Validation	Resilience Category 0-1 Supplier must test and validate the Data Recovery Plan(s) for each technology system/service required to support the delivery of services to Barclays and prove the recovery process can recover data to operational state. Validation should be performed at least once every 12 months. 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.
10. Platform and Application Rebuild plans	Resilience Category 0-1 Supplier must maintain a Platform and Application Rebuild Plan for each technology service/system required to support the delivery of services to Barclays and be subject to review, approval and testing at least once every 12 months. These plans are for situations where traditional recovery/restore options can't be used and the system needs to be rebuild from 'bare metal'. Plans should consider: • Operating system/infrastructure software	It is critical that technology services and support arrangements have appropriate recovery plans for a Cyber / Data Integrity event.

Control Title	Control Description	Why this is important
	• Application deployment and configuration • Security controls/configuration • System ecosystem dependencies and re-integration • Data Requirements (Data Recovery Plan) • Tooling dependencies to execute recovery plans 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).	