BARCLAYS

External Supplier Control Obligations

Recovery Planning

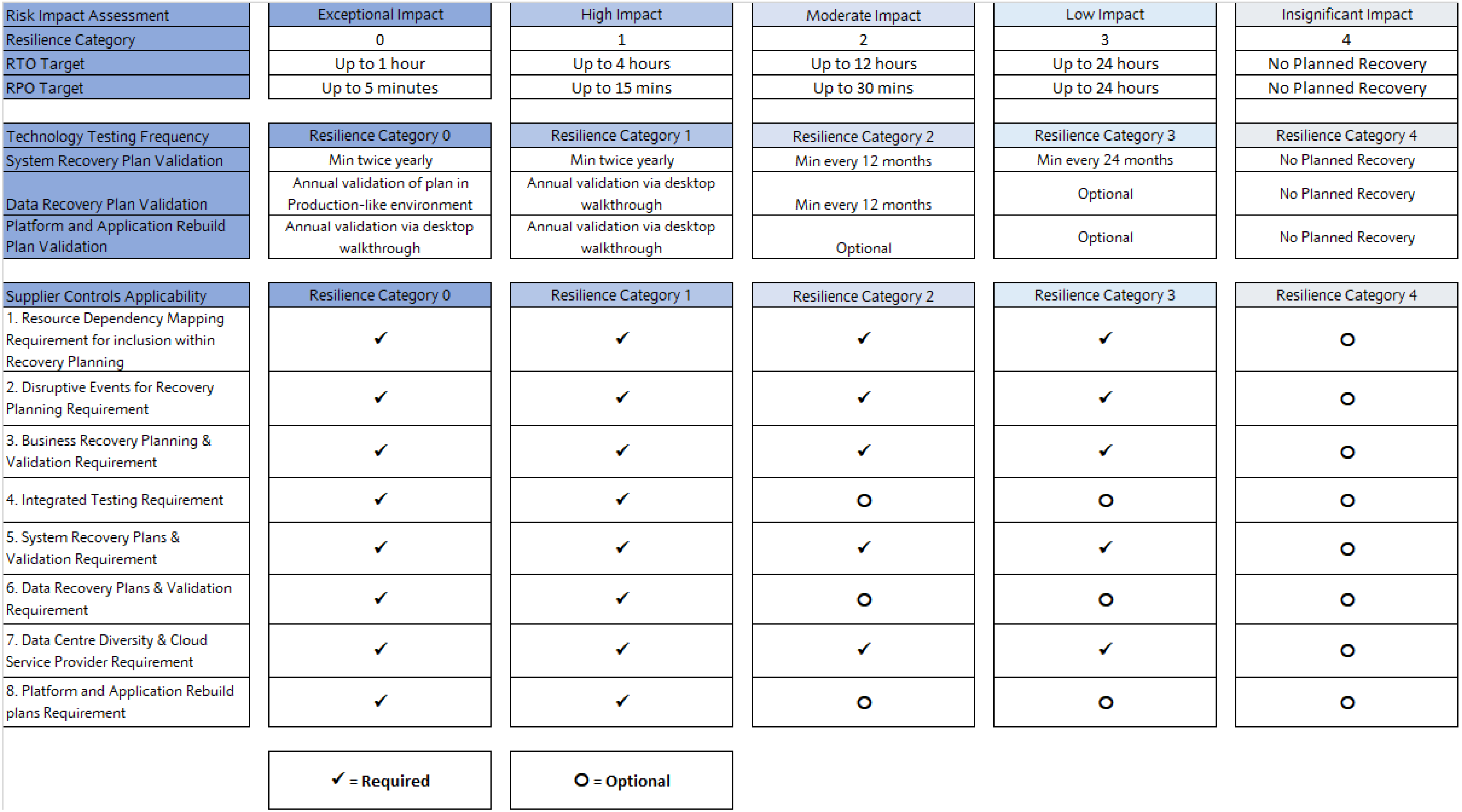
Version 14.0 FINAL October 2024

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. Disruptions such as cyber events, natural disasters, or man-made events can interrupt an entity's operations.
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.
Recovery Point Objective	The Recovery Point Objective (RPO) is defined as "the target status for the availability of data at the start of the recovery process". It is a measurement of the maximum data loss that is tolerable to the business in a recovery situation.
Resilience Category	Resilience Category is a rating used by Barclays to apply resilience requirements to a service based on criticality and impact. The Resilience Category drives Recovery Time Objective (RTO), Recovery Point Objective (RPO) and validation frequency requirement.
Intolerable Harm	The point at which disruption to Service becomes intolerable from the perspective of Customers/Consumers/Clients, financial markets or the safety and soundness of Barclays.
Resource Dependencies	Those dependencies (Technology, Third Party Service, Workforce) which are required to deliver the business Services.

2. Resilience Criticality Matrix:

Supplier's services are assigned to a specific Resilience Category (0-4) which reflects recovery objectives that Barclays requires the Supplier to meet based on the impact a disruption of the service may cause Barclays. A higher Resilience Category (i.e., lower number) will require a higher standard of resilience and recovery capability commensurate with the criticality of the service to Barclays. Supplier shall ensure that its services meet the recovery requirements as specified in the Resilience Criticality Matrix for the applicable Resilience Category stipulated by Barclays for the contracted services. The Resilience Criticality Matrix specifies which Controls are applicable based on Resilience Category. Details of the control requirement are set out at Section 3 (*Controls*).



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	Min every 12 months	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. Resource Dependency Mapping Requirement for inclusion within Recovery Planning	✓	✓	✓	✓	○
2. Disruptive Events for Recovery Planning Requirement	✓	✓	✓	✓	○
3. Business 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 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 assessed for effectiveness on an annual basis.

Control Title	Control Description	Why this is important
1. Resource Dependency Mapping Requirement for inclusion within Recovery Planning	Supplier must define and document resource dependencies which are critical to delivering the service to Barclays. These dependencies must be maintained and reviewed every 12 months or when material change occurs. Resource Dependences to consider include: ▪ Technology and data (internal and Subcontractor 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).	Suppliers need to understand and document their resource dependencies for providing their service to Barclays. Resource dependencies must form part of the Supplier's Business Recovery Plan to ensure these are considered to mitigate the impact of incidents and prevent the unavailability of the service to Barclays.
2. Disruptive Events for Recovery Planning Requirement	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 Disruption Events remain reflective of the current risk/threat landscape, are assessed for severity and plausibility, and are supported by industry and intelligence insights. As a minimum, the Supplier must include the following Disruption Events in the scope of its planning. ▪ Loss of building(s) across multiple locations impacting delivery of services to Barclays. (Buildings and associated infrastructure are unavailable). ▪ Loss of data scenario, including data corruption, 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). ▪ Loss of Material Subcontractor (Services or Supplies).	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).

Control Title	Control Description	Why this is important
	Disruption Events must be reviewed annually, and on a continuous basis, to inform planning and testing and demonstrate how this evolves over time.	
3. Business Recovery Planning & Validation Requirement	Supplier must maintain Recovery Plans for its defined Disruption Events to support its recovery targets. Recovery Plans should document the detailed recovery steps and Supplier responses which are possible to mitigate the impact and/or defer the unavailability of services provided to Barclays. As a minimum this should address: ▪ Possible workarounds. ▪ Decision Protocols. ▪ Communication and business prioritisation to resume/maintain a minimum viable service level. ▪ Dependencies. 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. 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).	Businesses are expected to have documented Recovery Plans in place and validation is completed to assure Barclays that the plans work as intended and include all dependencies to demonstrate that the agreed service levels can be delivered and that the services meet the resilience requirements stipulated by Barclays.
4. Integrated Testing Requirement	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.	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
	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.	There are regulatory requirements for Barclays to execute Business Continuity testing with third party service providers.
5. System Recovery Plans & Validation Requirement	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 Barclays Resilience Category. 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. (Minimum of one week) For services designed as active/active, validation should prove the ability to continue operating under the loss of a node, instance, or Availability Zone (for Cloud hosted) of the system (minimum 60 minutes). Validation frequency requirements are defined by the Resilience Category for the system. See the Resilience Criticality Matrix.	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 & Validation Requirement	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: ▪ Data sources and flow (upstream and downstream) ▪ Backup and replication sources ▪ Data synchronisation requirements post restore 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.	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.

Control Title	Control Description	Why this is important
7. Data Centre Diversity & Cloud Service Provider Requirement	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. 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.	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.
8. Platform and Application Rebuild Plans Requirement	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. These plans are for situations where traditional recovery/restore options can't be used, and the system needs to be rebuilt from 'bare metal'. Plans should consider: ▪ 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 and orchestrate recovery plans ▪ Recovery of Control Plane (E.G. Active Directory) Validation of the plan at a minimum must be evidenced by a table-top exercise to demonstrate feasibility.	It is critical that technology services and support arrangements have appropriate recovery plans for a Cyber / Data Integrity event.