BARCLAYS

External Supplier Control Obligations

Technology Risk

Version 10.0 Dated October 2020

Control Area	Control Title	Control Description	Why this is important
1. Managing obsolescence	Ensuring ongoing support arrangements	The supplier must promptly advise Barclays of known changes in their capability to provide support, whether direct or indirect, for IT assets used in the provision of services to Barclays including where products have security vulnerabilities, and must ensure timely upgrade or retirement of those IT assets.	Inadequate records and/or procedures on hardware and software assets going out of support or technology services becoming reliant on outdated hardware or software may lead to unacceptable performance, instability, security vulnerabilities, loss of business and excessive migration costs.
2. Incident Handling	Recording, classifying and resolving incidents	The supplier must operate a regime of incident handling in relation to the operation of its IT systems and services, that ensures all such operational incidents are appropriately identified, recorded, prioritised, classified and resolved promptly either at first contact or by timely and appropriate escalation. This must include a robust process for the prompt and effective handling of Major Incidents.	Technology incidents not reported in time or with sufficient detail, or where the necessary corrective action is not taken, may result in avoidable systems/service disruption, or data corruption or loss. Major Incidents require an enhanced and urgent response on the basis that they are Incidents that pose a significant risk to business and can result in serious consequences including severe outages, loss of reputation, financial impact and impact to core business processes.
3. Problem Management	Identifying, assessing/ analysing and resolving technology problems	The supplier must operate a regime of timely investigation into the problems underlying significant Technology incidents, which ensures identification and recording of such problems through root cause analysis, and their effective resolution to minimize the likelihood and impact of incident recurrence. The Supplier should also ensure that there is proactive analysis of routine incidents in order to identify and resolve the cause of common, high volume repeat incidents.	Where underlying problems giving rise to incidents impacting on Technology services provision are not identified and resolved in timely manner, they can lead to avoidable systems/service disruption, or data corruption or loss.
4. Change Management	Enforcing rigorous change control	The supplier must ensure that all IT components that are used in the provision of services to Barclays are managed under a rigorous change control regime, which takes full account of the following objectives:	Inadequate Change processes to prevent unauthorized, poorly managed or inappropriate changes to Technology services may lead to service disruption, data corruption, data loss, processing error or fraud.

		1. No change without appropriate authorisation - approval must take place prior to implementation 2. Segregation of duties between the change initiator, owner, approver and implementer 3. Changes planned and managed according to the level of associated risk 4. Changes take adequate account of potential impact on performance and/or capacity of affected technology components 5. Changes undergo technical and business testing relevant to the change prior to implementation, with evidence retained where required 6. Changes must be tested post implementation to ensure that they have been delivered successfully with no unplanned impact	
5a. Technology Resilience	System Recovery Plan (SRP)	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. **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	Absence or inadequate System Recovery Plans may lead to unacceptable loss of technology service to the Business or clients following an incident. Keeping resilience documentation updated and practiced ensures that recovery plans remain aligned to business needs.

5b. Technology Resilience	Data Integrity Recovery Plan (DIRP)	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 12 months.	Loss of data is one of the biggest threats we face as 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.
5c. Technology Resilience	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 single event.
5d. Technology Resilience	SRP Validation	Supplier must test and validate the System Recovery Plan(s) (SRP) to demonstrate that the technology systems/services can be recovered to meet the Resilience Category 0-3 requirements stipulated by Barclays. 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). Validation frequency requirements must be supported by the associated Resilience Category i.e.: - Resilience Category 0: SRP validation must be performed every 12 months and for PCO every 3 months	Supplier provided technology systems can impact Barclays customer journeys. Ensuring that suppliers 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.

		- Resilience Category 1: SRP and PCO validation must be performed every 12 months - Resilience Category 2-3: SRP validation must be performed 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). Supplier must notify Barclays prior to executing PCO.	
5e. Technology Resilience	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 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, recovery or recreate data must be exercised to confirm it is accurate and viable.
6. Performance and capacity Management	Remaining aligned to Barclays's technology needs	The supplier must define suitable levels of performance and capacity for all key IT components used in the provision of services to Barclays, in line with stated Business needs. They must also ensure that appropriate alerts and thresholds are in place on key components, to warn for potential breaching of thresholds, and that these are reviewed periodically to ensure service delivery is aligned to Barclays' needs.	Inadequate measures to monitor the performance and/or capacity levels of IT resources and failure to keep them in line with current and future requirements may lead to unacceptable reduction and/or interruption of Technology services and a loss of business. Inadequate definition and or documentation of Business/Clients needs may lead to unacceptable performance in Technology services and a loss of business.

Control Area	Control Title	Control Description	Why this is important
7. Technology Application Development	Enforcing repeatable quality assurance	The supplier must ensure that all It systems and services used in the provision of services to Barclays can be demonstrated to have undergone rigorous, thorough, and repeatable quality assurance processes including but not limited to functional and non-functional testing, static application security testing, and code quality assurance either through peer review or automated tooling.	Inadequately tested and quality assured systems and services may lead to unpredictable critical loss of functionality in technology services and business processes.
	Business outcome acceptance	The supplier must agree either on a one-off or an ongoing basis mutually acceptable business outcome definitions by which new or updated releases of IT systems and services are supplied to and accepted by Barclays. The form of these definitions must include sufficient functional and non-functional aspects of the systems and services, and may take any appropriate mutually agreed form such as existing system manuals, detailed mutually agreed requirements documentation, user stories, use cases or any other appropriate form. The supplier must work with Barclays to ensure that business outcomes either in whole or in mutually agreed part are accepted either on a one-off or an ongoing basis based on Barclays' business acceptance of these previously agreed definitions.	Inadequate agreement of system functional and non-functional behaviour may lead to deviation from expected Barclays' system behaviour leading to risk to business and operational processes.
8. Backup arrangements for systems and data	Operating appropriate and effective backup and restore processes	The supplier must ensure that all IT systems and services used in the provision of services to Barclays have adequate backup and restore processes in place that are operating in line with Barclays' needs and are periodically proven to be effective.	Absence or Poorly controlled business data back-ups may lead to systems/service disruption, data loss or inappropriate data disclosure.

	Ensuring safe, secure and reliable backup media	The supplier must ensure that all backup media associated with the provision of services to Barclays, together with the arrangements for the handling and storage of those media, remain both secure and reliable at all times.	Absence or Poorly controlled business data back-ups may lead to systems/ service disruption, data loss or inappropriate data disclosure.
9. Configuration Management	Isolating the Production Environment	The supplier must ensure that Production services provided to Barclays have no dependencies on any non-production components so that insecure or unreliable service delivery may be avoided.	Inappropriate register entries on technology components (hardware and software) including defined ownership and 3rd party dependencies may lead to insecure or unreliable services and data. The use of non-production components in the provision of production services creates risk in that they may not be built to or managed by production standards.
	Recording & Maintaining Configuration details	The supplier must maintain a complete and accurate register entry for all in-scope Configuration Items used in the provision of services to Barclays (including ownership and upstream/downstream dependencies/mappings). The Supplier must have controls in place that assure the ongoing maintenance of the accuracy and completeness of the data.	Inappropriate or incomplete register entries (together with related dependencies/mappings to other configuration items) can result in insecure or unstable services and data as a result of ineffective incident and change impact assessment.
10. Hardware Asset Management	Recording & Maintaining Hardware Asset details	The Supplier must have controls in place that assure the recording and ongoing maintenance of hardware asset data throughout the Asset's lifecycle. The supplier must maintain a complete and accurate register entry for all IT Hardware assets used in the provision of services to Barclays).	Inappropriate register entries on technology Hardware assets including defined ownership and 3rd party dependencies may lead to insecure or unreliable services and data. Failure to cleanse and dispose of Hardware Assets securely can lead to financial, reputational and regulatory damage.
	Asset Disposal	All disposed of Assets must be fully cleansed of all Barclays data and securely disposed of through a formal Disposal process, that aligns with the requirements of the relevant Barclays Security Standards.	Critical that supplier obtains and records formal confirmation that assets have been disposed of correctly (incl. safe destruction of bank data). Failure to cleanse and dispose of Hardware Assets securely can lead to financial, reputational and regulatory damage.

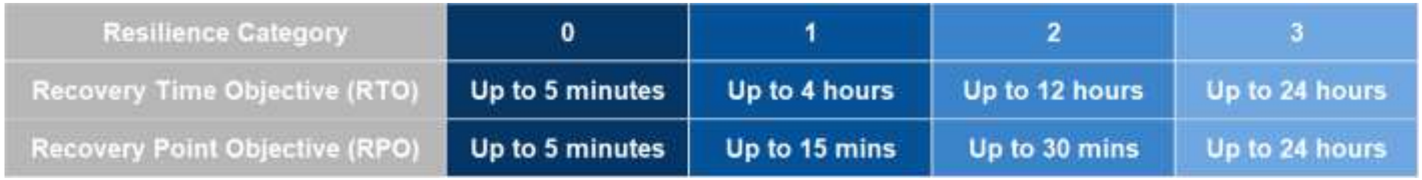
	Missing Assets	All ‘Lost or Stolen’ Assets must be properly investigated and reported to Barclays for risk sign-off if not found.	Critical that supplier has controls in place to assure that missing assets have been thoroughly investigated and – where not found – are reported to Barclays for risk sign-off. Loss and thus failure to cleanse and dispose of Hardware Assets securely can lead to financial, reputational and regulatory damage.

Control Area	Control Title	Control Description	Why this is important
11. Software Asset Management	Recording and Maintaining Software Asset/Installation details. Software Asset licensing	The supplier must maintain a complete and accurate register entry for all in-scope software assets and installations thereof used in the provision of services to Barclays (including ownership). The Supplier must maintain the accuracy and completeness of the data from procurement to disposal (and installation to deinstallation). The Supplier must also ensure that software usage remains in line with the terms of the defined Licence.	Inappropriate register entries on technology software assets including defined ownership may lead to insecure or unreliable services and data. Failure to manage software usage against entitlement can lead to financial, reputational and regulatory damage.

Technology Resilience Definitions:

Recovery Time Objective (RTO)	RTO is the time between an unexpected failure or interruption of services and the resumption of operations.
Recovery Point Objective (RPO)	RPO is 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 in a recovery situation.
Production Crossover (PCO)	PCO is the act of activating the alternate (DR) instance for systems designed in an Active-Passive configuration and using it as the production instance over an extended period of time to validate the full functionality and capability.
System Recovery Plan	A system recovery plan is a document that defines the technical elements and details for how to recover a system or any failed component back to an operational state.
Data Integrity and Recovery Plan	A Data Integrity and Recovery Plan is a document which states steps to be taken to recover lost data due to a system failure or a malicious intent. The plan should address scenarios with relevant options (E.G. Data play-back from other systems, Data Restore from tape archives, or recreation of data).

Barclays Resilience Requirements by Resilience Category Matrix



Resilience Category	0	1	2	3
Recovery Time Objective (RTO)	Up to 5 minutes	Up to 4 hours	Up to 12 hours	Up to 24 hours
Recovery Point Objective (RPO)	Up to 5 minutes	Up to 15 mins	Up to 30 mins	Up to 24 hours