BARCLAYS

External Supplier Control Obligations

Technology Risk

Version 9.0 Dated April 2019

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and/or procedures on hardware and software assets going out of support or technology services becoming reliant on outdated hardware or software may lead to unacceptable performance, instability, security vulnerabilities, loss of business and excessive migration costs.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 measures to monitor the performance and/or capacity levels of IT resources and 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. Also, inadequate Change processes to

		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	prevent unauthorized or inappropriate changes to Technology services may lead to service disruption, data corruption, data loss, processing error or fraud.
5. Service Continuity	Providing and validating suitable resilience / recovery arrangements	The supplier must understand and agree Barclays's resilience/recovery needs for each of the IT systems and services it provides to Barclays. Resilience and recovery plans should be maintained and confirmed as accurate and service continuity arrangements should be adequately documented and practiced/proven to be reliable and in line with business needs.	Absence or Inadequate service continuity planning 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.
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 definition and or documentation on 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 maintain 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 maintain a complete and accurate register entry for all in-scope IT Hardware assets used in the provision of services to Barclays (including ownership and labelling where required). The Supplier must maintain the accuracy and completeness of the data throughout the Asset's lifecycle from procurement to 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.	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.

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 Hardware 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.