BARCLAYS

External Supplier Control Obligations

Technology Risk for Proof of Concepts*

Reduced Proof of Concept Controls Obligations to be applied only when directed by Barclays
Version 9.0 Dated April 2019

Control Area	Control Title	Control Description	PoC Inclusion
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.	Not in scope for PoC
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.	Only relevant for POC if the IT system is hosted by supplier (or their third-party) and if the platform will host confidential data.
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.	Not in scope for PoC
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: 1. No change without appropriate authorisation - approval must take place prior	Not in scope for PoC

		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	
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.	Not in scope for PoC
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.	Not in scope for PoC

Control Area	Control Title	Control Description	PoC Inclusion
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.	Only relevant for POC if the IT system is hosted by supplier (or their third-party) and if the platform will host confidential data.
	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.	Not in scope for PoC
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.	Only relevant for POC if the IT system is hosted by supplier (or their third-party) and if the platform will host confidential data.

	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.	Only relevant for POC if the IT system is hosted by supplier (or their third-party) and if the platform will host confidential data.
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.	Not in scope for PoC
	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.	Not in scope for PoC
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.	Not in scope for PoC

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.	Not in scope for PoC