External Supplier Control Obligations

Technology Risk – Technical Controls

Version 12.0 Dated October 2022

Control Area	Control Title	Control Description	Why this is important
1. Problem Management	Problem Identification and Recording	The Supplier must ensure that timely root cause investigation is undertaken for all one-off Major Incidents, and repeat Incidents where the combined impact is sufficient to cause significant operational impact.	Where the root cause of significant Incidents is not identified and resolved in a timely manner, the service remains at risk of repeat and avoidable failures, leading to systems/service disruption, reputational damage and/or data corruption/loss
	Problem Management and Resolution	The Supplier must ensure that the root cause of significant Incidents is fixed in a timely manner or – where this is not possible – risk-acceptance is provided from Barclays and appropriate mitigating controls are applied to limit the likelihood of a recurrence.	

Control Area	Control Title	Control Description	Why this is important
2. 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, including the following requirements: 1. No changes may be made without appropriate authorisation from Barclays prior to implementation. 2. There must be segregation of duties between the change initiator, owner, approver and implementer. 3. Changes must be planned and managed according to the level of risk	Inadequate change processes to prevent unauthorized, poorly managed or inappropriate changes to technology may lead to service disruption, data corruption, data loss, processing error or fraud.

		associated with maintaining the minimum required level of service to Barclays. 4. Changes must take adequate account of potential impact on performance and/or capacity of affected technology components. 5. Changes must 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.	
3. Performance and capacity Management	Remaining aligned to Barclays' technology needs	The Supplier must define, maintain and document suitable levels of performance and capacity for all key IT components used in the provision of services to Barclays, in line with all contractual requirements. 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 meet all contractual requirements and Barclays' needs.	Inadequate measures to define, document and 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.

Control Area	Control Title	Control Description	Why this is important
4. Technology Application Development	Testing Strategy and Completion prior to Technical and/or Business go-live	The Supplier must understand the quality of all software before selling or supplying that software to Barclays. All software code must be in version control system(s) and signed off by the Supplier Service Provider before it is provided to Barclays. Application changes must undergo software testing by the Supplier to ensure the software meets captured requirements. Testing evidence must be retained.	Inadequately tested and quality assured systems and services may lead to unpredictable critical loss of functionality in technology services and business processes.
	Confirming System Requirements	When delivering software to Barclays' specifications, the Supplier must ensure that business requirements are clearly defined and agreed with Barclays.	Inadequately defined business requirements may lead to incorrect system behaviour, leading to risk to business and operational processes.
	Business Acceptance prior to Deployment	When delivering software to Barclays' specifications, the Supplier must agree and follow a quality/acceptance process which has been agreed with Barclays.	Inadequate business acceptance prior to deployment may lead to incorrect system behaviour, leading to risk to business and operational processes.

5. 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 of 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 secure and reliable at all times.	Secure and reliable back-up media are necessary to avoid systems/ service disruption, data loss or inappropriate data disclosure.

Control Area	Control Title	Control Description	Why this is important
6. 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.	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 Items	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.
7. Service Level Management	Defining and monitoring Service Performance	The Supplier should ensure the service complies with the agreed service levels, including service level monitoring and reporting.	Service levels ensure that IT Services are delivered in line with agreed IT service commitments

Technology Definitions:

Configuration Item	Any component that needs to be managed in order to deliver an IT service. Configuration Items can be physical (e.g., a computer or router), virtual (e.g., a virtual server) or logical (e.g., a service). Changes (additions, modifications or cessations) must be undertaken under the control of change management.
Incident	An unplanned interruption to an IT Service or a reduction in the quality of an IT Service, including, without limitation the failure of a Configuration Item that has not yet impacted a service.
IT Service	A Service provided to one or more Customers by an IT Service Provider. An IT Service is made up from a combination of people, processes and IT and is provided to customers to support their Business Processes.
Major Incident	An Incident that poses a significant risk/impact to Barclays and can result in serious consequences including severe loss of productivity, reputational / regulatory damage and impact to core business processes, key controls or systems.
Problem	The unknown cause of one or more Incidents.