External Supplier Control Obligations

Technology Risk – Technical Controls

Version 14.0 Dated October 2024

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 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 the Incidents described above 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. The Supplier must inform Barclays of all Significant Changes prior to its implementation so that impact assessment can be undertaken and appropriate mitigating actions put in place as required. 2. There must be segregation of duties between the change initiator, owner, approver and implementer.	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.

		3. Changes must be planned and managed according to the level of risk 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, taking into account known business demand and current capacity utilisation to ensure that available capacity continues to meet 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 ensure the software/service performs as the supplier has described before selling or supplying that software or software based service to Barclays or provide a view of known defects and impact to delivery of the software/service. All software code must be in version control systems and signed off by the Supplier before it is provided to Barclays. The Supplier must subject all application changes to software testing to ensure the software meets captured requirements. The Supplier must retain testing evidence.	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 technology 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 business 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.

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.
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.
Significant Changes	Changes which will impact – or which have the potential to impact – the effective operation of the service(s) provided to Barclays, and/or changes for which Barclays will or may need to undertake appropriate risk mitigating actions in support of their implementation.