WOOLWORTHS FINANCIAL SERVICES

WFS Supplier Control Obligations- Technology Risk

Control Area	Control Title	Control Description	Why this is important
Managing obsolescence	Ensuring Ongoing support arrangements.	The supplier must promptly advise WFS of known changes in their capability to provide support, whether direct or indirect, for IT assets used in the provision of services to WFS 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and/or procedures on hardware and software assets going out of support or technology services becoming reliant on outdated hardware or software may lead to unacceptable performance, instability, security vulnerabilities, loss of business and excessive migration costs. WFS has low appetite for loss and or significant disruption to business activities from the unavailability, underperformance, recoverability or obsolescence of technology.
Incident Handling	Recording, classifying and resolving incidents.	The supplier must operate a regime of all technically related incident handling in relation to the operation of its IT systems and services, that ensures all such operational incidents are appropriately identified, recorded, classified and either promptly resolved or escalated as necessary as per the documented service criteria.	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. Continually assessing the lifespan of the components of its technology systems, whilst planning for their replacement as they age.
Problem Management	Identifying, assessing/analyzing 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.	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.

Control Area	Control Title	Control Description	Why this is important
Configuration Management	Maintaining complete and accurate technology configuration records.	The supplier must maintain complete and accurate register entries in respect of all the technology components (hardware and software) used in the provision of services to WFS, together with the information necessary for their ongoing support, and ensure all such entries remain up to date. Collectively, all such technology components are referred to as "Production Environment".	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.
Configuration Management	Isolating the production Environment.	The supplier must ensure that all production IT systems and services used in the provision of services to WFS must not comprise, make use of or be accessed by components that are not in the production environment. The production environment must only host a system / device that has previously undergone development and testing in the other environments.	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.
Configuration Management	Exercising source code management.	The supplier must ensure that source code and scripts/utilities relating to the provision of services to WFS, such as those that enable event-monitoring, batch processing, reporting, file transfers etc., (latest and previous versions) are appropriately recorded in CMDB tool and must be managed to support service delivery and continued enhancement under change control. The source code must be provided in an escrow account by the supplier and updates must be provided to the organisation when changes are made on the systems.	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.

Control Area	Control Title	Control Description	Why this is important
Service Continuity	Providing and validating suitable resilience / recovery arrangements.	The supplier must understand and agree WFS's resilience/recovery needs of each of the IT systems and services it provides to WFS, and ensure its service continuity arrangements are adequately practiced/proven to be reliable. Results from DR exercises must be documented, evaluated and reported to relevant stakeholders.	Absence or Inadequate service continuity planning may lead to unacceptable loss of technology service to the Business or clients following an incident.
	Managing the data centre environment.	The supplier must ensure that environmental and physical security arrangements surrounding those data centres involved in the provision of services to WFS are adequately established, managed and controlled.	Absence or Inadequate service continuity planning may lead to unacceptable loss of technology service to the Business or clients following an incident.

Control Area	Control Title	Control Description	Why this is important
Backup arrangements for systems and data	Operating appropriate and effective backup processes.	The supplier must ensure that all IT systems and services used in the provision of services to WFS have adequate backup processes in place that are operating in line with WFS's needs and periodically proven to be effective. Restoration of these backups is regularly tested, on an individual and collective basis, against defined recovery time objectives (RTO) and recovery point objectives (RPO).	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 WFS, together with the arrangements for the handling and storage of those media, remain both secure and reliable at all times. Ensure the Group can recover from a technology failure or disaster it regularly establishes immutable backups of applications and database.	Absence or poorly controlled business data back-ups may lead to systems/service disruption, data loss or inappropriate data disclosure.
Performance and capacity Management	Remaining aligned to WFSs technology needs	The supplier must define suitable levels of performance and capacity for all key IT components used in the provision of services to WFS and undertake regular monitoring to ensure service delivery is and remain aligned to WFS's needs.	Inadequate definition and or documentation on Business/Clients needs may lead to unacceptable performance in Technology services and a loss of business
Change Management	Enforcing rigorous change control.	The supplier must ensure that all IT components that are used in the provision of services to WFS 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 prevent unauthorized or inappropriate changes to Technology services may

Control Area	Control Title	Control Description	Why this is important
		° No change without appropriate Authorization. ° Segregation of duties between the change initiator/implementer and approver. ° Changes planned and managed according to the level of associated risk. ° Changes take adequate account of potential impact on performance and/or capacity of affected technology components. ° All changes to be fully approved before they can be implemented. ° Rights to modify the Production environment are limited to only those requiring those rights to fulfil their role. ° Changes undergo technical and business testing relevant to the change, with evidence retained. ° Testing is performed in a dedicated environment appropriate to the test requirements and the planned test activities. ° Change is accompanied by sufficient user training and appropriate updates to system, user and procedural documentation.	lead to service disruption, data corruption, data loss, processing error or fraud.