WOOLWORTHS FINANCIAL SERVICES

External Supplier Control Obligations
EUDA – End User Developed Applications

Version 8 May 2020

Control Area	Control Title	Control Description	Why this is important
Governance and Assurance	Roles and Responsibilities	The Supplier must define and communicate roles and responsibilities for EUDA's. These must be reviewed after any material change to the Supplier's operating model or business. Key roles must include a senior executive, accountable for EUDA's.	EUDA's require high-level sponsorship to ensure that controls are designed, implemented, and operated effectively. Ongoing monitoring is necessary to provide senior management with assurance over the design and operation of information risk controls.
	Information Risk Reporting	Documented controls and processes must be in place to ensure EUDA Risk Incidents are reported and managed. EUDA Incidents and information breaches should be responded to by the Supplier and reported to WFS immediately. An incident response process for timely handling and reporting of errors impacting WFS' Information and/or Services used by WFS should be established. The Supplier must ensure that identified remedial actions following an incident are addressed with a remediation plan (action, ownership, delivery date) and shared and agreed with WFS.	
	On-going Monitoring	The Supplier must regularly and in any event not less than once in every calendar year, measure, review and document its compliance with this Schedule.	
	Adherence to local legislative and statutory requirements	The Supplier must ensure that EUDA related legislative and statutory requirements which apply to the jurisdiction in which the Supplier operates are appropriately documented and complied with.	
Education and Awareness	New Joiner education and awareness	The Supplier must ensure that all new Supplier Personnel with EUDA responsibilities are identified and, within a reasonable time, complete training which ensures they understand their EUDA roles and responsibilities.	To ensure that all Supplier Personnel with EUDA responsibilities understand their responsibilities to prevent the Supplier from inadvertently exposing EUDA's and the information they contain to avoidable risks.
	On-going education and awareness	The Supplier must ensure that Employees identified with EUDA responsibilities provided education and awareness appropriate to their role (a) at a frequency suitable to the importance of their responsibilities, and (b) not less often than once per year.	
EUDA Control Objectives	Identification and Criticality Assessment	A process must be documented and in place to identify all EUDAs that support WFS' services. The Criticality of the EUDA must be agreed with WFS.	Identification and criticality assessment of EUDAs is paramount in determining the right level of control required for all EUDAs.

EUDA Control Objectives	Minimum Control requirements Based on EUDA criticality	The EUDA Primary User must implement controls that satisfy the requirements of the control objectives based on the criticality level agreed with WFS. Evidence must be retained, where appropriate, to demonstrate the applicable controls objectives are being achieved.	The correct level of control must be applied in line with the risk represented by the EUDA to avoid excessive control on a lower risk EUDA
EUDA Control Objectives	Registration	A EUDA inventory must exist to provide transparency of the complete in scope EUDA population for the supplier as well as capturing key attributes to support the provisions of this Schedule. A process must be documented and in place to ensure a complete, accurate and up-to-date inventory of EUDAs. The EUDA inventory must be reviewed at least annually to maintain accuracy and verify completeness.	The completeness of the EUDA inventory is fundamental to ensure the proper security and operation of EUDAs
EUDA Control Objectives	Access	Access to data and business logic for all EUDAs must be restricted to appropriate users with the appropriate access rights. Access must be reviewed using a risk-based approach.	Appropriate access controls protect EUDAs from unauthorised, inappropriate, or unattributable access.
EUDA Control Objectives	Availability	Controls must be in place to ensure that EUDAs must be available in line with BUs requirements.	The availability of EUDAs ensures continuous operation of business processes.
EUDA Control Objectives	Change management	Following change management principles ensures that EUDAs are operating as expected following business logic changes.	Appropriate change management is vital for the EUDA to continue to function as expected after any change
EUDA Control Objectives	Transition to a managed application	The EUDA owner must have a process in place to consider on an annual basis the potential transition of high criticality rated EUDAs to a managed technology solution.	Moving Critically rated EUDAs onto Managed applications would improve the controls in the process, as well as improve efficiency, as this allows more standardized controls to be implemented.

Definitions	
EUDA Owner	Every EUDA must have a named EUDA Owner. The EUDA Owner is accountable for: • Maintain a complete and accurate inventory of all EUDAs for their respective teams; and • Confirm all EUDAs within their Ownership comply with the provisions of this policy. Confirm that transition of high criticality rated EUDAs to a managed technology solution is considered annually
EUDA Primary User	Every EUDA must have a named EUDA Primary User. The EUDA Primary User is responsible for: • Confirm integrity of the data, calculations, and all other content in the EUDA. • Identify and registration of EUDA with the appropriate EUDA inventory. • Complete of the Criticality Assessment for the EUDA. • Support on-going development and maintenance of the EUDA; and Confirm that the EUDA satisfies the control objectives defined in this policy.
EUDA Reviewer	Responsible reviewer must be an individual, other than the Primary User, with sufficient knowledge and experience of the EUDA to be able to: • Support the on-going use and maintenance of the EUDA in the absence of the EUDA Primary User; and Support key control activities that would require independent review.
EUDA User	Responsible individual who is using a EUDA is a EUDA user and is responsible to be aware and uphold the provisions of this policy and standard.
Business logic	The portion of the EUDA which determines how data is transformed or calculated to support the purpose of the EUDA.
Structural Changes	Changes defined as; Worksheets added/deleted; Worksheet protection change; VBA Macro change; VBA Reference change; Link's change; Data Connection change; Access rights change; Properties change; Named range change.