WOOLWORTHS FINANCIAL SERVICES

External Supplier Control Obligations
Payments Process

Version 8 Dated August 2021

Title	Control Description	Why this is important
Adherence to local legislative and statutory requirements	The Supplier must ensure that legal and regulatory requirements which apply to the payments which the Supplier processes are appropriately documented and complied with.	To ensure that payments are processed in accordance with both legal and regulatory requirements in scope. Failure to comply with legal and regulatory requirements could results in fines and reputational issues.
Material Payments Process Risk Identification	The Supplier must review the list of payments processes to ensure that all the risks are identified, managed, and monitored accordingly.	This requirement ensures proactive identification of material payments process risks and implementation of key controls to manage the risks.
Manual Payment inventory list	The Supplier must identify all manual payments processing to ensure that all the risks associated with manual payments processing are identified, managed, and monitored accordingly. A process must be documented and in place to ensure a complete, accurate and up-to-date inventory of manual payments in a way to support the provisions of this Schedule. A manual payment inventory (MPI) list must exist to provide transparency of the complete in scope manual payments process for the supplier as well as capturing key attributes to support the provisions of this Schedule. The MPI must be reviewed at least annually to verify and maintain accuracy and completeness.	If this requirement is not implemented, WFS may not be able to gain confidence that the Supplier has adequate documented procedures to respond to risk associated with manual payments processes. The requirement behind the MPI ensures that the Supplier Manager has performed an end-to-end review to identify any manual payment processes and eventually implement and monitor any required key controls associated with the risk of processing manual payments. This may reduce the risk of associated loss, reputational damage and/or regulatory fine/censure.
Integrity of payment instruction	The supplier must ensure that the payments instructions integrity is maintained throughout the payment lifecycle. The Supplier must have the minimum key controls in place to maintain and protect the authenticity and integrity of the instructions. This includes that the instruction: • Cannot be modified and remains in its original state from initiation to settlement • is processed and settled accurately, i.e., in line with the original request and applicable regulations • is not duplicated	If this requirement is not implemented, WFS may not be able to gain confidence that Supplier has the adequate controls to ensure that the integrity of the payments instructions is maintained throughout the payment cycle. This may result in potential fraudulent payments, payments being processed inaccurately and associated reputational damage and/or regulatory fine/censure.

Control Title	Control Description	Why this is important
Authentication Checks: Authentication of sender	The supplier must ensure that the payment request is genuine. The supplier should confirm that the payment request is from a legitimate source (e.g. 'ID&V' checks); and confirm the validity of the payment instructions' integrity	This requirement confirms the l legitimacy of the payments instructions by ensuring that the payment instruction is genuine. This control decreases the risk of loss associated with fraudulent payments, associated reputational damage and/or regulator fine/censure.
Authorization Checks: Authority of the sender	The Supplier must ensure that each payment request has been approved by the pre-defined and pre-approved individuals.	This requirement confirms the genuineness of the payments instructions by ensuring that the signatories on the pa yenta instructions are mandated to do so. This control mitigates the risk of loss associated with fraudulent payments, associated reputational damage and/or regulator fine/censure
Authorization Checks: Authorization throughout payment life cycle	The supplier must ensure that, through the payment life cycle, that the person approving the payment is doing so within the set Limits of Authority (pre-defined and pre-approved Limits of authority). The Limits of Authority should be reviewed on at least an annual basis or as and when required.	This requirement confirms the validity of the payments instructions by ensuring that the different level of authority provided throughout the payment process is aligned with the business established and approved delegation of authority. This control mitigates the risk of loss associated with fraudulent/inaccurate payments, associated reputational damage and/or regulator fine/censure
Segregation of Duties: Independent levels throughout payment life cycle	The supplier must ensure that the person approving the payment is independent and has no access to create or amend the instruction.	This control ensures that any potential inaccuracy or any potential issues are proactively identified by an independent Indi visual. This control decreases the risk of loss associated with fraudulent/inaccurate =e payments, associated reputational damage and/or regulator fine/censure
Payment service levels and performance monitoring: Delays in payment processing	The Supplier must ensure that each payment is processed and settled on a timely manner to ensure that the SLAs are met (customer and schemes requirements)	This requirement ensures that all payments being processed by the supplier are processed in accordance with the applicable payments/card schemes cut off as well as in according to the customer requirements. This in turn reduces the risk of having payments processed with delays. Delayed processing of payment instructions may result in increased customer dissatisfaction and complaints, leading to potential customer attrition and reputational damage.

Payments Reconciliations	The Supplier must ensure that payment reconciliation controls are implemented to ensure that payments are processed accurately, settled in a timely manner, debits and credits agree and that discrepancies are investigated and corrected.	This control ensures that any potential inaccuracy or any potential issues are proactively identified and resolved. This control also decreases the risk of loss associated with fraudulent/inaccurate payments, associated reputational damage and/or regulator fine/censure
Eligible method of communication and transmission methods to transfer payments instructions	The Supplier must ensure that all eligible communication and transmission methods to transfer payments instructions are scrutinized to ensure that the appropriate levels of controls are implemented.	WFS has defined prohibited, restricted, and approved methods of transmitting payments instructions to mitigate the multiple risks such as information risk (Data Privacy), fraud risk (manipulation of data), cyber risk (cyber threats) etc. Restricted communication methods are to be used only when adequate controls are in place
Roles and Responsibilities	The Supplier must define and communicate roles and responsibilities for payments process risk. These must be reviewed after any material change to the Supplier's operating model or business.	This requirement ensures that the roles and responsibilities of both ends are established, documented and approved. This will assist in case of dispute .
Payment / Card Scheme Risk	Payment / Card Scheme Risk collaboratively refers to the three main risk categories associated with membership to a payment / card scheme, scheme's structure and operations: • Business risk • Settlement risk • Operational risk In instances where the third-party provider is a member (direct/indirect) of any payment/card scheme, the scheme owner should ensure that any materialized business/settlement or operational risk, specifically related to timeliness as well as regular assessment, is reported through established governance channels. The Supplier must review the list of payments/card schemes to ensure that all the risks are identified, managed and monitored accordingly. The Supplier must review the list of payments/card schemes to ensure that all the risks are identified, managed and monitored accordingly.	The control provides the context to what a payment/card scheme risk refers from an WFS perspective. This will ensure that the definition of payment/card scheme risk is clearly understood for proactive identification and ownership of manual payments processing together with proper risk management. Through this requirement, the supplier must ensure that any materialized business/settlement or operational risk, specifically related to timeliness as well as regular assessment, is reported through established governance channels. This will ensure timely actions are undertaken to mitigate any operational issues including legal and reputational risk. If this requirement is not implemented, WFS may not be able to gain confidence that the Supplier has ensured complete coverage of the requirements.

Control Title	Control Description	Why this is important
Payment / Card Scheme Risk	The Supplier must ensure that all payments processed on behalf of WFS are processed in compliance with the Payment/Card Scheme requirements.	If this requirement is not implemented, WFS may not be able to gain confidence that the Supplier has adequate documented procedures to respond to risk associated with non-compliance with the payment/card scheme requirements. Any payments processed inaccurately, with delays, with authentication failures or with authorization failures and leading to non- compliance with the applicable payment regulations must be reported against the associated Level 3 risks. Additionally, any non-compliance to payments regulations must follow the relevant governance process for reporting regulatory breaches under Conduct Risk.
Scheme Risk Assessment	The Supplier must perform a comprehensive scheme risk assessment at least on an annual basis, for each payment/card scheme for which it holds direct and indirect membership. The risk assessment needs to be signed off by the scheme owner and senior management	This control requirement aims at ensuring that the 3 main risks associated with the payment/card scheme have been managed accordingly. Non proper assessment may result in potential fraudulent payments, payments being processed inaccurately and associated reputational damage and/or regulatory fine/censure
Due Diligence	Prior to taking a new membership or sponsorship in a payment/card scheme, the Supplier needs to perform a formal due diligence to ensure that the minimum requirements are covered.	This requirement ensures that the supplier has performed the required level of due diligence to reduce the risk of loss associated with fraudulent payments, associated reputational damage and/or regulator fine/censure.
Change	In the event of significant changes to processes or regulations, the supplier must perform an additional out of cycle risk assessment to ensure that the scheme risk is being managed in accordance with the WFS framework for Payment Schemes.	This control requirement aims at ensuring that the 3 main risks associated with the changes related to the payment/card scheme have been managed accordingly. Non proper assessment may result in potential fraudulent payments, payments being processed inaccurately and associated reputational damage and/or regulatory fine/censure

Control Title	Control Description	Why this is important
Scheme Owner	The Supplier must ensure that a payment/card scheme owner is designated to maintain the overall relationship and ensuring ongoing risk monitoring of scheme arrangement. Additionally, the Supplier must ensure that the scheme owner monitors and reports the scheme risk as per governance channels	This requirement ensures that the relevant payment/card scheme has a designated owner to better manage the relationship and to ensure timely reporting.
Incident Management and Response Levels associated with manual payment errors	The Supplier must proactively report any failure in the operations of manual payments processes linked to internal or external fraud, human error, system issues or inadequate processes.	To ensure timely escalation of operational issues linked to manual payments errors as well as proactive identification to mitigate customer and operational impact.
Incident reporting	Documented process must be in place to ensure that all operational failures including Payments Process risk incidents, together with the volumes and value of the payments impacted, and customers and Business Unit impacted are reported on a timely basis to WFS. Incidents 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 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.	An incident response process helps to ensure that incidents are quickly contained and prevented from escalating. If this requirement is not implemented, WFS may not be able to gain confidence that Supplier has adequate documented and tested procedures to respond to payments incidents. This may lead to inappropriate action being taken following an incident, increasing the risk of loss, or associated reputational damage and/or regulatory fine/censure. Having an established documented and approved procedure for managing and reporting operational failures will ensure completeness of reporting as well as identification of lessons learnt (if any) with other Business Units (BUs).
Ongoing 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.	On-going assurance maintains the control environment at the supplier

Acronyms	Definitions
Payments Process Risk	Payments Process Risk refers to the risk of payments being processed inaccurately, with delays, without appropriate authentic action and authorization. In the context of PPR, a payment is defined as inward, outward, or internal transfer * of funds from one party to another (client/customer/counterparty/employee/ third parties, etc.) that is settled via an external scheme or correspondent banking relationship. It includes payments processes from initiation through to external settlement, including any repairs or amendments.
Manual	Anything that involves human intervention anywhere within the end-to-end transaction/ payments process lifecycle.
Manual Payment	A manual payment is the inward, outward, or internal transfer of funds from one party to another that is settled via an external scheme or correspondent banking relationship whereby any part of the payment process from initiation through to settlement, including a Ny repair or amendment, is manual.
Manual Payment Risk	Manual Payments Risk relates to a failure in operation of manual payment processes because of internal or external fraud, human error, system issues or inadequate processes
Eligible method of communication and transmission methods to transfer payments instructions	Prohibited methods are: External Drives/USB/ Floppy Disks/ CDs/Diskette Restricted methods: Branch/In person/ Fax/Email /Telephone/Verbal/Paper/Spreadsheets and EUC's* Eligible methods are: Online banking, Mobile banking, Other defined and agreed methods within the approved appetite * Note on Restricted methods: these channels can be used if appropriate controls as per the policy are in place.
Payment life cycle	Commences at the initiation and capture of the payment in the payments channel and ends when the payment is settled with counterparty via external settlement system.
Sender	An individual that submits payment request(s).
Payment / Card Scheme Risk	• Payment / Card Scheme Risk collaboratively refers to the three main risk categories associated with membership to a payment / card scheme, scheme's structure, and operations: • Business risk: The risk that the payment / card scheme / system or any of its components - for example, an infrastructure provider serving it - cannot be maintained as a going concern in the face of adverse financial shocks. • Settlement risk: The risk that another participant in a scheme cannot or does not meet its financial obligations when, under the rules of the scheme, they fall due; or that another institution that facilitates the settlement of those obligations -such as the settlement agent - becomes insolvent. • Operational risk: The risk that a system operator or core provider to the scheme is operationally unable to process or settle payments as intended from inadequate or failed internal processes, people, and systems.