External Supplier Control Objectives for Nationwide Technology Risk

Version – 1.0

Risk Appetite

This external supplier control objectives document is designed to ensure that the Society's suppliers operate within the risk appetite set by the Society's Board.
The Control Objectives contained in this document are critical measures of success for the Risk Appetite Statements.

Control Objectives

Control Objective	Control Requirement	Control Description	Why is it important to Nationwide
Incident Handling & Problem Management	Record, classify and prioritise incidents.	The supplier must operate a robust process for the handling of incidents in relation to the technology services being provided to Nationwide. All relevant information must be recorded so incidents can be handled effectively, and are identified, recorded, prioritised, classified and resolved in accordance with the Service Level Agreements and the Society's risk appetite. A full historical record must be maintained and available for a minimum of 13 months. Suppliers must have a reporting process to immediately alert the supplier manager at Nationwide of any incident that may impact the ability to continue the provision of the service.	The management of technology incidents and problems are critical to provide efficient, effective, and timely resolution of all types of technology incidents to minimise business and member disruption and to maintain member expectations of service. The objective of Incident Management is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. 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. Major Incidents require an enhanced and urgent response on the basis that they are Incidents that pose a significant risk to business and can result in serious consequences including severe outages, loss of reputation, financial impact and impact to core business processes. 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.
	Problem Management - identifying, assessing/ analysing, and resolving technology problems	Suppliers 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. The Supplier should also ensure that there is proactive analysis of routine incidents to identify and resolve the cause of common, high volume repeat incidents. Root cause determination and remediation for service impacting incidents must be tracked to conclusion and consider 'read-across' issues in other technology services. This 'read across' must include reporting to the Nationwide Supplier Manager any incidents for other clients that have the potential to also impact technology service provided to Nationwide Building Society.	

Managing & Maintaining Technology Assets	Ensuring ongoing support arrangements	Suppliers must promptly advise Nationwide of known changes in their capability to provide support, whether direct or indirect, for technology assets used in the provision of services to Nationwide including where products have security vulnerabilities and must ensure timely upgrade or retirement of those technical 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.
	Hardware asset management - Recording & Maintaining Hardware Asset details	Suppliers must have controls in place that assure the recording and ongoing maintenance of hardware asset data throughout the asset's lifecycle. Suppliers must maintain a complete and accurate register entry for all technology hardware assets used in the provision of services to Nationwide. Where necessary the asset records must be shared with Nationwide for the completeness of the Nationwide Configuration Management System (CMS).	Inappropriate register entries on technology Hardware assets including defined ownership and 3rd party dependencies may lead to insecure or unreliable services and data. Failure to cleanse and dispose of Hardware Assets securely can lead to financial, reputational, and regulatory damage
	Hardware asset management – Asset disposal	All disposed of Assets must be fully cleansed of all Nationwide data and securely disposed of through a formal Disposal process, that aligns with the requirements of the relevant Nationwide Security Standards	It is critical that suppliers obtains and records formal confirmation that assets have been disposed of correctly (incl. safe destruction of building society data). Failure to cleanse and dispose of Hardware Assets securely can lead to financial, reputational, and regulatory damage.
	Hardware asset management – Missing assets	All 'Lost or Stolen' Assets must be properly investigated and reported to Nationwide for risk sign-off if not found.	It is critical that suppliers have controls in place to assure that missing assets have been thoroughly investigated and – where not found – are reported to Nationwide for risk sign-off. Loss and thus failure to cleanse and dispose of Hardware Assets securely can lead to financial, reputational, and regulatory damage.
	Software asset management - Recording and Maintaining Software Asset/Installation details. Software Asset licensing	Suppliers must maintain a complete and accurate register entry for all in-scope software assets and installations thereof used in the provision of services to Nationwide (including ownership). Suppliers must maintain the accuracy and completeness of the data from procurement to disposal (and installation to deinstallation). Suppliers must also ensure that software usage remains in line with the terms of the defined Licence.	Inappropriate register entries on technology software assets including defined ownership may lead to insecure or unreliable services and data. Failure to manage software usage against entitlement can lead to financial, reputational, and regulatory damage.

Change Control	Enforcing rigorous change control	Suppliers must ensure that all IT components that are used in the provision of services to Nationwide are managed under a rigorous change control regime, which takes full account of the following objectives: 1. All technical change that may impact the service provision to Nationwide must coordinated with Nationwide and approved according to the appropriate risk 2. No change without appropriate authorisation - approval must take place prior to implementation 3. Segregation of duties between the change initiator, owner, approver, and implementer 4. Changes planned and managed according to the level of associated risk 5. Changes take adequate account of potential impact on performance and/or capacity of affected technology components 6. Changes undergo technical and business testing relevant to the change prior to implementation, with evidence retained where required 7. Changes must be tested post implementation to ensure that they have been delivered successfully with no unplanned impact	Inadequate Change processes to prevent unauthorized, poorly managed, or inappropriate changes to Technology services may lead to service disruption, data corruption, data loss, processing error or fraud
Managing and Maintaining Configuration Management	Isolating the Production Environment	Suppliers must ensure that Production services provided to Nationwide have no dependencies on any non-production components so that insecure or unreliable service delivery may be avoided.	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. 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 details	Supplier must maintain a complete and accurate register entry for all in-scope Configuration Items used in the provision of services to Nationwide (including ownership and upstream/downstream dependencies/mappings). Suppliers must have controls in place	Inappropriate or incomplete register entries (together with related dependencies/mappings to other configuration items) can result in

<table>
<tr><td></td><td></td><td>that assure the ongoing maintenance of the accuracy and completeness of the data. Where necessary the Configuration Item records must be shared with Nationwide for the completeness of the Nationwide Configuration Management System (CMS).</td><td>insecure or unstable services and data because of ineffective incident and change impact assessment.</td></tr>
<tr><td rowspan="2">Backup arrangements for systems and data</td><td>Operating appropriate and effective backup and restore processes</td><td>Suppliers must ensure that all technology systems and services used in the provision of services to Nationwide have adequate backup and restoration processes in place that are operating in line with Nationwide needs and are periodically proven to be effective.</td><td rowspan="2">Absence or poorly controlled business data backups may lead to systems and service disruptions, data loss or inappropriate data disclosure.</td></tr>
<tr><td>Ensuring safe, secure, and reliable backup media</td><td>Suppliers must ensure that all backup media associated with the provision of services o Nationwide, together with the arrangements for the handling of stoae of those media always remain both secure and reliable.</td></tr>
<tr><td>Performance and Capacity Management</td><td>Remaining aligned to Nationwide technology needs</td><td>Suppliers must define suitable levels of performance and capacity for all key IT components used in the provision of service for Nationwide, in line with stated business needs. They must also ensure that appropriate alerts and thresholds are in place on key components to want for potential breaching of thresholds, and that these are reviewed periodically to ensure service delivery is aligned to Nationwide needs.</td><td>Inadequate measures to monitor the performance and or capacity levels of the technology resources and failure to keep them in line with current and future requirements maty lead to unacceptable reduction and or interruption of Technology Services and loss of business.

Inadequate definition and or documentation of Nationwide needs may lead to unacceptable performance in technology services and loss of business.</td></tr>
<tr><td>Technology Resilience</td><td>System and Data recovery assurance</td><td>Suppliers must have Recovery Plan(s) for each technology system/service required to support the delivery of Nationwide Business and Internal service lines and the corresponding Recovery Time Objectives (RTO) and Recovery Point Objective (RPO). Plan(s) must be reviewed for accuracy at least once every 12 months.
<table>
<tr><td>Rating</td><td>RTO</td><td>RPO</td></tr>
<tr><td>Core</td><td>4 hours</td><td>Up to 2 minutes of data loss</td></tr>
<tr><td>Premium</td><td>4 hours</td><td>Up to 2 minutes of data loss</td></tr>
</table></td><td>Absence or inadequate Recovery Plans may lead to unacceptable loss of technology service to the Society or Members following an incident. Keeping resilience documentation updated and practiced ensures that recovery plans remain aligned to business needs.</td></tr>
</table>

<table>
<tr>
<td></td>
<td></td>
<td>
<table>
<tr><td>Enhanced</td><td>8 hours</td><td>Up to 6 hours of data loss</td></tr>
<tr><td>Standard</td><td>24 hours</td><td>Up to 12 hours of data loss</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Centre Diversity</td>
<td>Suppliers must ensure that each technology system/service required to support the delivery of Nationwide Business and Internal service lines are resilient across data centres and far apart enough to reduce the risk of data centres being impacted simultaneously by a single event.
<table>
<tr><th>Rating</th><th>On Prem, IaaS & PaaS- DR Provision</th><th>Saas Providers</th></tr>
<tr><td>Core</td><td>Active/Active</td><td rowspan="4">Nationwide operates Cloud SaaS Principles, ask for latest principles.</td></tr>
<tr><td>Premium</td><td>Active/Active</td></tr>
<tr><td>Enhanced</td><td>Dedicated DR provision to match production</td></tr>
<tr><td>Standard</td><td>DR configuration must be available in DR location with compute and storage added by automation as required</td></tr>
</table>
</td>
<td>Data Centres should have alternate power sources, network links, etc. and be far apart enough to reduce risk of data centres being impacted simultaneously by single event.</td>
</tr>
<tr>
<td></td>
<td>System and data recovery validation</td>
<td>Suppliers must test and validate the Recovery Plan(s) to demonstrate that the technology systems/services and data can be recovered to meet the requirements stipulated by Natiowndie.

Validation frequency requirements must be supported by the associated Business and Internal service lines Resilience rating

Resilience Category Platinum: validation must be performed every 12 months

Resilience Category Gold, Silver & Bronze: validation must be performed every 24 months

If any testing fails to achieve the minimum recovery requirements for the applicable Resilience Category, supplier must promptly notify Natiowide and provide detailed remediation plans (including actions to be undertaken and corresponding completion dates).</td>
<td>Supplier provided technology systems can impact Nationwide member journeys. Ensuring that suppliers that support Nationwide business operations have adequate resilience plans that are tested is crucial and also a Regulatory mandate for Nationwide to apply proper governance in managing our suppliers.

Data is a critical element that can be adversely impacted in many ways. The documented plan to restore, recovery or recreate data must be exercised to confirm it is accurate and viable.</td>
</tr>
</table>