GROUP TECHNOLOGY POLICY

SUMMARY FOR THIRD PARTY SUPPLIERS

RATIONALE

Group Policy Rationale

The purpose of this Policy is to assist the Group **to deliver Technology which meets customer expectations, supports Group strategy and complies with all applicable laws and regulations**.

In addition, this Policy has been designed to support compliance with the following regulations and / or guidelines:

1. FCA Handbook: Systems and Controls
2. PRA Supervisory Statement on Outsourcing and Third-Party Risk Management
3. EBA Guidelines on ICT Operational and Security Risk Management
4. EBA Guidelines on Outsourcing Arrangements

The following requirements clarify the outcomes which are intended to be achieved through the Group's Suppliers compliance with its Technology Policy.

SCOPE

All suppliers where they provide, maintain and/or support technology (regardless of where the technology is hosted) which is used by the Group must adhere to the 3rd party policy.

Out of scope

Technology used solely by the supplier for conducting its own day to day business in the delivery of services to the Group or its customers and is fully managed by the supplier is out of scope (this is covered under the Operational Resilience Policy).

Technology which is supplied and hosted entirely on LBG premises, where the operation of controls and all activities are undertaken only by LBG colleagues is out of scope (this is covered under the internal LBG Technology Policy).

THIRD PARTY POLICY REQUIREMENTS

1. TECHNOLOGY STRATEGY, DESIGN & GOVERNANCE

1.1 All elements of externally supplied technology services, including onward supply chain relationships, must meet the requirements of contractual agreements.

1.2 Suppliers must ensure that technology processes, applications and systems are compliant with legal and regulatory requirements for UK and International jurisdictions relevant to technology services provided to LBG.

1.3 Identified operational risks (including operating models) and high and critical vulnerabilities with a potential impact to the technology service must be notified to the LBG Supplier Manager together with a mitigation / remediation action plan.

1.4 Technology services provided to LBG by suppliers must be designed, built tested, implemented, and maintained to meet approved LBG requirements, where relevant.

2. TECHNOLOGY BUILD, DEVELOPMENT OR ACQUISITION

2.1 Suppliers must report to the LBG Supplier Manager in a reasonable timeframe ahead of implementation for full consultation where new technology is adopted and/or a change is made to existing technology that changes how the technology service is provided.

2.2 Where Open Source software has been used this must be documented and approved by LBG, ensuring that documentation covers all relevant aspects, including vulnerability scanning, licencing, supportability and exit planning. This assessment should include any skills or ongoing support required.

3. TECHNOLOGY CHANGE & DEPLOYMENT

3.1 Suppliers must ensure that all changes are robustly controlled, managed through an IT Service Management Tool and subject to risk and impact assessment, tested (including functional and non-functional testing) and approved by the Supplier Manager.

3.2 All technology changes must have an approved recovery plan in place prior to change implementation, with requirements for full back-out plans risk assessed and agreed with LBG.

3.3 Potential change conflicts must be assessed in conjunction with LBG and prioritised to minimise risk to production business services.

3.4 Testing environments must be separated from production environments and mirror live production. Critical Business Processes (CBP) and Important Business Services (IBS) supporting services must have separate, segregated test environments that mirror the state, volume, and complexity of production.

3.5 Test plans must be formally documented and approved, with evidence of testing outcomes ahead of implementing changes. All technical changes for Group services must have an approved recovery plan in place prior to implementation, with requirements for full back-out plans risk assessed and agreed with LBG where there is potential to impact critical services.

3.6 Post-testing, software must be released using defined software release mechanisms, which must be automated, where possible, to control production changes.

3.7 Suppliers must ensure that software code and configuration provided to LBG as a service is stored in a strategic/enterprise repository and utilise automated enterprise deployment mechanisms across all environments.

4. END TO END TECHNOLOGY ASSET MANAGEMENT

4.1 Suppliers must identify and maintain technology assets that are critically required to deliver LBG Critical Business Processes (CBP) and Important Business Services (IBS).

4.2 Suppliers must ensure that technology assets that are critically required to deliver LBG's Critical Business Processes and Important Business Services are mapped, depicting the flow of data at rest, in transit and in memory within 3rd and LBG 4th parties for the service they provide.

4.3 All, asset(s) must be recorded in a database. This includes the configurations for hardware, software, services (e.g. cloud services) and networks. It applies to newly installed systems as well as for operational systems over their lifetime. The interdependencies of assets must be recorded and monitored to reduce any potential impacts these may cause in the event of an incident.

4.4 Suppliers must ensure that an inventory of all software (including for Cloud, cloud deployed software licences being consumed) must be discoverable using automated processes/tools where possible and support ongoing maintenance of the technology asset inventory.

4.5 Suppliers must ensure that the choice of repository is appropriate and allows technology to be operated or changed when required and must utilise enterprise toolsets, ensure it covers run, change and recover requirements and reviewed every 12 months or after significant change.

5. TECHNOLOGY CURRENCY

5.1 IT hardware and software currency, where this is the sole or joint responsibility with a supplier, must be kept at version levels that allow the supplier and LBG to support, maintain, secure and/or patch where required. This includes full patching of vendor updates.

5.2 A roadmap must be in place with a clear line of sight of software / hardware version support dates (including vendor-supplied technology).

6. TECHNOLOGY CAPACITY AND PERFORMANCE

6.1 The performance of technology must be continually monitored, including component IT systems and batch schedules to prevent, detect and respond to performance issues.

6.2 Forecasting and analysis of business requirements and impacts (including future capacity requirements) must be used to plan and implement actions to reduce risk and maintain service availability.

6.3 End-to-end capacity must be monitored in line with business appetite. In addition, for Cloud technology, resource-level and application and tooling capacity with auto-scaling rules (where appropriate) must be designed, configured and maintained.

6.4 Technical procedures required to run, change and recover the end-to-end technology stack must be stored in an enterprise repository and reviewed every 12 months or after significant change.

6.5 Manual processes and single points of failure should be avoided. Where this is not possible these should be assessed with mitigations in place to manage the associated risks and documented within design documentation and considered for future automation.

6.6 Strategic scheduling and, where applicable, file transfer tooling must be utilised to initiate and track all batch jobs.

6.7 Performance and capacity monitoring plans and processes must be in place to prevent and respond to issues and capacity shortages.

6.8 Documented procedures to catchup and recover batch processing, including dependencies and successors, must be able to enable an optimised restoration of service after a disruption is in place and reviewed every 12 months or after significant change.

6.9 Batch Management processes must be reviewed to ensure there is appropriate space and time to recover from service incidents and include coding which is resilient and can be restarted to protect batches.

7. TECHNOLOGY MONITORING & RESPONSE

7.1 Suppliers must ensure technical procedures required to run, change, and recover the end-to-end technology stack for LBG services are indexable, searchable and reviewed with LBG every 12 months or after significant change.

7.2 Suppliers must have proactive monitoring and alerting in place to prevent, detect and respond to issues, including batch processing and any non-standard event in the application / service and allow sufficient time to recover from service incidents.

7.3 Assessment of monitoring logs must be carried out and documented continuously, alongside any major changes to business infrastructure, processes, or procedures. This must assess both current and forecasted performance and include known or predicted changes in volume to ensure sufficient capacity is maintained for continued service at utilisation above predicted peak workloads, including operating in disaster recovery configurations.

7.4 All incidents which could impact technology services supplied to LBG must be reported. Root cause determination and remediation for service impacting incidents and problems must be tracked to conclusion and consider ‘read-across’ issues in other technology services. This ‘read across’ must include reporting to the LBG Supplier Manager any incidents for other clients that have the potential to also impact technology service provided to LBG.

7.5 Incident trend analysis must be performed to enable efficient resolution and remediation. For major incidents, escalation rules and procedures must be defined, and suppliers must maintain an incident knowledge source including logs of past incidents.

7.6 Suppliers must ensure that continuous monitoring and log analytic systems are in place for the end-to-end technology stack of the IT system to maintain service provision performance, integrity of execution, timely response to system alerts and recovery from incidents.

7.7 Recovery from technology service incidents and problems must be timely to meet service level agreements and remain within LBG risk appetite for LBG Critical Business Processes or Important Business Services and LBG Business Impact Assessment availability requirements. The supplier must

ensure the required levels of support for the service provided is available to LBG during BAU and incident response in a timely fashion.

8. TECHNOLOGY RESILIENCE AND RECOVERY

Backup & Restore

8.1 Suppliers must ensure that Technology services critical to LBG are designed and configured to be resilient, highly available and recoverable. These services include Critical Business Process and Important Business Services, which must be maintained in line with LBG IT resilience requirements and/or Business Impact Assessment (BIA) availability requirements and must be reviewed at least annually. Platforms must be hosted in highly resilient data centres or deployed on cloud services with characteristics that are at least equivalent.

Key aspects include:

8.2 Backup processes and business requirements must be agreed at least annually, as a minimum. These must specify the following:

- Backup designs must be configured to restore service to a point in time that provides minimal and acceptable levels of data loss to the business within Impact Tolerance thresholds.
- Backup design must be reviewed by relevant backup teams every 12 months or following a significant change to ensure that they are optimised to provide the most efficient restoration times.
- Back-out plans must be tested and proven where possible to recover technology services and avoid consequential impacts. Support documentation required by LBG must be provided for change implementation, post-live operational running, and service recovery.
- Suppliers must review the completeness and integrity of backups every 12 months or following a significant change and ensure service can be restored following a data loss or corruption event.
- Backups should be verified regarding their completeness and timeliness through clear reporting to key stakeholders.
- All Backups must be protected in line with their Confidentiality rating.

Restore Testing

8.3 Backup restoration procedures of the end-to-end IT System must be proven on a scheduled basis.

8.4 Backup restoration testing must be conducted in a non-production environment which has a similar state, volume and complexity of data as compared to production.

8.5 Testing must cover the restoration of the end-to-end technology stack (including the verification and validation of data and transactions) of the service (application code/configuration, databases) to ensure that the recovered system will function properly within the agreed impact tolerance in the event of a live event.

8.6 Detailed restoration testing results, including timings, issues encountered and path to mitigation, must be documented and published.

8.7 Suppliers must ensure backup restoration procedures contain steps to recover all LBG data and technology after a data loss or corruption event.

8.8 These back up and restoration procedures must be approved and reviewed every 12 months or following a significant change. Suppliers must deploy a backup design that enables an optimised recovery of data and the end-to-end technology stack which aligns to LBG backup restoration time and restoration point objectives.

8.9 Suppliers must review the completeness and integrity of data held in and restored from backup with LBG stakeholders every 12 months or following a significant change to ensure service can be resumed following a data loss or corruption event, including ransomware attack.

8.10 Data required to provide LBG services must be backed up and available at an approved secondary location which must not be located within 10 kilometres of the main site accessing the data. Where specific backup and recovery requirements are needed, these must be captured as local procedures.

8.11 Suppliers must ensure all backups of LBG data are encrypted, where technically possible, at rest and in transit to ensure they are impervious to accidental or malicious deletion or compromise.

8.12 Where backup encryption is not possible, the supplier implements measures to protect backups from accidental or malicious deletion or compromise.

8.13 Detailed restoration testing results for LBG services, including Backup Restoration Time and Point capabilities achieved, issues encountered and path to mitigation, must be provided to LBG stakeholders within 4 weeks of testing. Test results must be validated by comparing restored test systems to production systems to ensure data integrity and completeness and shared with the LBG Supplier Manager.

Disaster Recovery

8.14 Suppliers must prove IT Disaster Recovery (ITDR) plans and procedures in line with LBG's availability and integrity requirements (as determined by the Business Impact Assessment (BIA) or LBG resiliency requirements) or following a material IT change. New implementations must undertake ITDR proving (including LBG connectivity) within 4 weeks of service commencement. All proving outcomes must evidence that recovery can be achieved on target recovery infrastructure in line with LBG objectives in line with the agreed Recovery Time Capability (RTC), Recovery Point Capability (RPO) and Recovery Time Objective (RTO)

- Suppliers must perform scenario assessments for complex or high-risk restoration recovery scenarios where restoration proving is not possible.
- Results of backup scenario assessments must be documented and reviewed with LBG stakeholders.
- Suppliers must understand the ITDR RTO/RPO and proving frequency requirements with LBG for provision of the technology service. The frequency of recovery testing must be determined by the RPO and RTO for each system, with IBSs and CBPs tested at least annually. Testing of ITDR must be conducted in live production on the service directly provided to

LBG. Any failed disaster recovery proving, and remediation action required must be notified to the LBG Supplier Manager or relevant Business contact within 48 hours of the failure. Recovery proving must be retested successfully within 3 months of the failure. All test results must be documented, including any issues encountered.

- Suppliers must retain multiple skilled SMEs to support the run, change and recover activities of the end-to-end technology systems that provide LBG service provision.
- Supplier technology systems that support LBG IBS and CBP systems must have a support matrix in place detailing current and required skills for all critical information assets in their technology stack.

The Key Controls should be adhered to based on the services provided by the third party.

KEY CONTROLS		
Control Title	**Control Description**	**Frequency**
Technology services are developed in accordance with Group requirements	• Sign off from the Group is obtained for technology solutions prior to implementation for Group services.	Ad hoc
Separate test environments are established	• An environment definition document (or equivalent) and a master test plan (or equivalent) are in place for projects impacting Group services. • A readiness check is performed by the environment owner to confirm that the functional test environment is reflective of the live environment or a justification for it not reflecting live is documented	Ad hoc
Functional and non-functional testing is performed	• Functional and non-functional testing (to documented requirements) for projects impacting Group services is performed. • Test plans must be formally documented and approved prior to the commencement of testing. • End of test reports are made available for review and approval, prior to commencement of live deployments	Ad hoc
Technical support documentation	• Technical documentation, user manuals recovery processes etc. for all Group services exists and are reviewed on an annual basis or following a change	Annually
Change standard and tooling	• A standard for managing the implementation of technology change is in place and is reviewed annually. • An IT Service Management application or tool is used to manage technology changes	Annually Ad hoc
Implementation and back out plans for technical change	• All technical changes for Group services have an approved recovery plan in place prior to implementation,	Ad hoc

	with requirements for full back-out plans risk assessed and agreed with LBG where there is potential to impact critical services.	
Emergency change	• An emergency change process is documented. • Emergency changes are approved as per process.	Ad hoc
An IT incident & problem management process is fully implemented	• A process for Incident & Problem Management is documented. • All incidents & problems are logged, prioritised and assigned to the relevant teams for timely response and investigation. • Incidents & problems are tracked to resolution based on severity	Ad hoc
Currency management procedures are in place	• A Currency Management process (hardware and software) is defined and reviewed annually. • All Group supporting applications/systems currency is reviewed in accordance with the process. • All currency issues are logged and tracked to remediation	Annually Annually Ad hoc
Hardware and software inventories are in place	• An asset inventory is in place for the technology service provided to LBG and is updated following technology changes and contains configuration data, age of systems, and type of vendor support. • The inventory is reviewed on an annual basis.	Ad hoc
Batch jobs are created, prioritised and scheduled	• Ensure procedures are in place for the design, development and scheduling of batch jobs impacting Group services • Monitoring of the creation, prioritising, scheduling and execution of batch jobs must be in place	Ad hoc
Alerts are prioritised and configured in line with alerting requirements	• Alert monitoring requirements are defined and approved. • Alerts are configured and prioritised in line with defined requirements. • Continual monitoring of alerts for all Group systems is in place and issues are identified and tracked to resolution.	Ad hoc
Capacity management procedures are in place and executed	• A Capacity Management process, including configuration, must be documented, approved and reviewed annually • Capacity Management processes must be operating for Group systems, with	Annually Ad hoc

	alerts managed and trend analysis performed.	
Backup and restoration processes are in place and tested.	• Backup and restoration processes are in place and tested. • Backup and restoration processes are in place and reviewed annually. • Testing of backup and restoration processes to prove data recovery is undertaken.	Annually Annually Ad hoc
IT DR proving programme for systems, environment and core technology infrastructure which is provided in line with the proving schedule	• RTC and RPC for the system has been published by the Supplier. • RTC & RPC meet RTO & RPO requirements as specified by the Group • IT DR has been carried out in live production. • Failed disaster recovery proving and remediation action required must be notified to the LBG Supplier Manager or relevant Business contact within 48 hours. • Recovery proving must be retested successfully within 3 months of the failure.	Annually (Every 12 months)

2.6 Definitions

Technology Service(s)	Refers to the technology related elements of the service provided by the supplier, including IT systems, infrastructure, software, applications, networks, capabilities, processes and people.
Suppliers	Direct third party suppliers including those suppliers using downstream third party Suppliers who support the provision of technology services to Lloyds Banking Group
Important Business Services (IBS)	A service that LBG provides that delivers a specific outcome to one or more external customers or clients, and if disrupted or unavailable could; • pose a risk to the safety and soundness of Lloyds Banking Group, undermine policy holder protection, or cause instability in the UK financial system • cause intolerable harm to one or more of Lloyds Banking Groups customers or clients Further information on IBS can be found in the Minimal Operational Resilience Standards expected of third Party suppliers providing goods and services to Lloyds Banking Group.
Recovery Time Capability	The amount of time taken to switch from the primary system to a disaster recovery system from the point of recovery invocation

Recovery Point Capability	The amount of data loss measured in time following the failure of a system
Recovery Time Objective	The time required to switch from the primary system to a disaster recovery system from the point of recovery invocation.
Recovery Point Objective	The acceptable amount of data loss measured in time following the failure of a system

MANDATORY REQUIREMENTS – NON COMPLIANCE

Any differences between the requirements set out above and the supplier's own controls should be raised by the Supplier with Lloyds Banking Group's Supplier Manager.

The Supplier Manager will then discuss the non-compliance with the Accountable Executive for the relationship and local Risk team to agree way forward.

Version Number	Effective Date
1.0	30th November 2017
2.0	30th July 2018
3.0	1st January 2020
4.0	4th July 2022
4.1	January 2023
5.0	10th January 2024