LLOYDS BANKING GROUP	**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 legislation, regulations and / or guidelines:

1. Senior Management & Certification Regime (SM&CR)
2. FCA Handbook: Systems and Controls
3. PRA Rulebook: Capital Requirement Regulation / Solvency II Firms
4. PRA Supervisory Statement on Outsourcing and Third Party Risk Management
5. EBA Guidelines on ICT Operational and Security Risk Management
6. EBA Guidelines on Outsourcing Arrangements

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

PRINCIPLE
Principle 1 – Technology Governance We govern technology with clear accountabilities aligned to the Group's strategy. Technology is governed with clear accountabilities and in a timely manner and aligned to the Group's strategy.
Principle 2 – Build, Change & Acquisition We develop technology services robustly managed from quality design through to safe implementation following secure by design principles.
Principle 3 – Availability & Recovery We provide optimised and highly resilient technology services for our customers, colleagues, and the wider financial services market.
Principle 4 – Operation & Performance *We maintain delivery of business services through efficient and effective technology operations which are supported* and maintained *by automated processes and procedures.*

It is expected that Group suppliers will adhere to these principles and will provide their products and services in a manner that supports and enables the Group to uphold them.

GROUP TECHNOLOGY POLICY SUMMARY FOR THIRD PARTY SUPPLIERS

SCOPE

All suppliers where they provide, maintain and/or support technology (regardless of where the technology is hosted) which is used by the Group, or its customers should 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)

MANDATORY REQUIREMENTS - GENERAL

2.1 TECHNOLOGY GOVERNANCE

2.1.1 Contractual	All elements of technology service, including supply chain relationships, must meet the requirements of contractual agreements and schedules of work.
2.1.2 Legal and Regulatory	Technology processes, applications and systems must be compliant with legal and regulatory requirements for UK and International jurisdictions relevant to technology services provided to LBG.
2.1.3 Operational Risk Management	Operational risks (including operating models) with a potential impact to the technology service must be notified to the LBG Supplier Manager together with a mitigation / remediation action plan.
2.1.4 New Technology	Adoption of new technology services supporting LBG services, including Cloud technology and/or a change to existing technology that changes how the technology service is provided, must be highlighted to the LBG supplier manager for full LBG consultation in a reasonable timeframe ahead of implementation. This enables LBG to enact any contractual actions within its right and ensure compliance with any regulatory and other such obligations ahead of the change taking place.

2.2 BUILD, CHANGE AND ACQUISITION

2.2.1 Design and Build	Technology services must be designed, built tested, implemented and maintained to meet LBG approved requirements. Where Open Source software has been used this must be documented in Product Design documentation and approved by LBG, including that it covers all relevant aspects, including vulnerability scanning, licencing, supportability and exit planning
2.2.2 Technology Change Management	IT changes to technology services must be robustly controlled with changes risk and impact assessed, tested (including functional and non-functional testing) and approved. All changes and required approvals must be managed through an IT Service Management tool. Separate technology environments must be in place to ensure adequate segregation of duties and to mitigate the impact of unverified changes to production systems. Potential change conflicts must be assessed in conjunction with LBG and prioritised to minimise risk to production business services. Support documentation required by LBG must be provided for change implementation, post-live operational running and service recovery.
2.2.3 Technology Change Recovery Planning	IT 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. Back-out plans must be tested and proven where possible to recover technology services and avoid consequential impacts.

2.3 AVAILABILITY AND RECOVERY

2.3.1 Service Hosting Environments	All Technology services including those that are critical to a LBG Critical Business Process or Important Business Service, i.e. break the service chain, should be designed and configured to be resilient, highly available and recoverable. Platforms must be located in highly resilient data centres or deployed on cloud services with characteristics that are at least equivalent.
2.3.2 Technology Resilience	Technology service resilience must be maintained to meet LBG Business Impact Assessment availability requirements. Where a technology service supports and/or is part of an LBG Critical Business Process or Important Business Services must be maintained in line with LBG IT resilience requirements and subject to ongoing review at a minimum annually and for any changes.
2.3.3 Technology Currency	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 (as per contractual obligations) and LBG to support, maintain, secure and/or patch where required.

2.3.4 Backup and Restoration	Backup and restoration procedures for data and technology must be in place to ensure recovery. The scope, frequency and testing of backups must be in line with the LBG recovery requirements.
2.3.5 Disaster Recovery Capability & Testing	IT disaster recovery must be proven in line with LBG's availability and integrity requirements (as determined by the business impact assessment) or following a material IT change. New implementations must undertake DR 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 i.e.: • Recovery Time Capability (RTC) meets the Recovery Time Objective (RTO) • Recovery Point Capability (RPC) meets the Recovery Point Objective (RPO) • Data required to provide LBG services must be backed up and available at an approved secondary location IT disaster recovery RTO/RPO and proving frequency requirements must be detailed in the contract for provision of the technology service. Where an annual test is required, this must be undertaken every 12 months. The IT DR 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.
2.3.6 Technology Service Incident and Problem Management	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. 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.

2.4 OPERATION AND PERFORMANCE

2.4.1 Asset and Configuration Management	An up-to-date, accurate and complete record of technology assets must be maintained for the technology service provided to LBG (for example: hardware, software, licences, source code and versioning).

	This must include the configuration of the assets (for example, age, type of vendor support etc.) and the links and interdependencies between the different assets.
2.4.2 Service Management	Operational procedures must be in place to support consistent delivery of technology service to LBG and ongoing maintenance of technology and recovery capability in accordance with laws and regulations, technical and business requirements and vendor specifications.
2.4.3 Operational Monitoring	Continuous monitoring must be in place for the technology service, component IT systems and batch schedules, to maintain service provision performance, integrity of execution, timely response to system alerts and recovery from incidents.
2.4.4 Capacity Management	Capacity of IT systems must be monitored to ensure sufficient capacity is maintained and forecasting undertaken to ensure continued service at utilisation above predicted peak workloads, including operating in disaster recovery configurations.
2.4.5 Automation of Manual Processes	Operational processes should be automated to remove manual activities and repetitive tasks to improve efficiency and reduce the risk of human error.
2.4.6 Batch Management	Batch jobs must be scheduled and managed for all batch jobs, with automation and auto-scaling where appropriate. Monitoring of the creation, prioritising, scheduling and execution of batch jobs must be in place. Any batch overruns that have occurred must have had the underlying cause identified and remediated.

.

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

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

GROUP TECHNOLOGY POLICY SUMMARY FOR THIRD PARTY SUPPLIERS

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, with requirements for full back-out plans risk assessed and agreed with LBG where there is potential to impact critical services.	Ad hoc
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
Backup and restoration process are in place and tested.	• Backup and restoration process are in place and reviewed annually. • Testing of backup and restoration processes to prove data recovery is undertaken.	Annually Adhoc
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

GROUP TECHNOLOGY POLICY SUMMARY FOR THIRD PARTY SUPPLIERS

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 alerts managed and trend analysis performed	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)

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