GROUP TECHNOLOGY POLICY

SUMMARY FOR THIRD PARTY SUPPLIERS

1.0 RATIONALE

Group Policy Rationale

The purpose of this Policy is to support 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

Customer Impact

These policy principles underpin technology provision within the Group and align to the following risk themes for Technology:

- **Governance** – Effective technology governance is in place with clear accountabilities to manage group impacting and systemic risks and deliver strategic business objectives, regulatory and legal requirements.

- **Build, Change and Acquisition** – Development of technology solutions has a well-managed lifecycle from quality design through to safe implementation.

- **Availability, Performance and Recovery** – Optimised and highly resilient technology services are provided to run critical business processes for our customers, colleagues and the wider financial services market.

- **Operation** – Efficient and effective technology processes maintain delivery of business services within expected operating thresholds and risk appetite.

1.1 SCOPE

This Policy Summary applies to third party suppliers to Lloyds Banking Group as follows:

- **IT Disaster Recovery requirements** (sections 2.3.4 & 2.3.5) apply to **all suppliers hosting technology used by the Group or its customers**.
- Suppliers who are **hosting bespoke technology off Group premises used by the Group or its customers** where the third or a fourth party is managing the implementation of controls - including providing this technology using an externally managed cloud service, including Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).

Only those key controls relevant to the technology service being provided to or for the Group need to be operated.

The table below provides additional information to understand the policy scope.

The following suppliers/services are out of scope of this Policy Summary:

- Third party suppliers where they are acting as a Technology Provider to or for the Group and their technology is hosted on Group premises where LBG are managing the implementation of controls.
- LBG internally managed cloud services or public cloud services used by LBG where LBG are managing the implementation of controls.

Note: IT Disaster Recovery for technology used solely by the Supplier for the delivery of services to the Group is out of scope of this policy if it is not used by the Group or its customers (as this is covered under the Resilience & Continuity Policy).

Service Hosting	Service Criteria	Policy Requirement	Applicability
Technology Service Hosting – Off Group Premises	Third party supplier of technology used by the Group or its customers	IT Disaster Recovery (sections 2.3.4 & 2.3.5)	All suppliers
	Commercial Off The Shelf technology (COTS) solutions, i.e. not bespoke to LBG	IT Disaster Recovery (sections 2.3.4 & 2.3.5)	All suppliers
	Third party supplier of technology used by the Group or its customers that provides a bespoke service to LBG, where the third (or fourth) party is managing the implementation of controls	All policy requirements	All applicable suppliers
	Third party supplier of technology used by the Group or its customers that provides a bespoke service to LBG, and is an externally managed cloud service, including: • Software as a Service (SaaS) • Infrastructure as a Service (IaaS) • Platform as a Service (PaaS)		
	LBG internally managed cloud services	Not in Policy scope	N/A
	Public cloud services used by LBG, where LBG are managing the implementation of controls		
Technology Service Hosting – On Group Premises	Third Party supplier using remote access capabilities to manage the technology provided by the supplier	All policy requirements	All applicable suppliers
	Third Party technology services where LBG are managing the implementation of controls (except where the supplier has remote access capability)	Not in Policy scope	N/A

2.0 MANDATORY REQUIREMENTS

The following requirements, applicable from the date of Policy publication are intended to support management of technology risk by third party suppliers:

2.1 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 with a potential material impact to the technology service must be notified to the LBG Supplier Manager together with a mitigation / remediation action plan.
2.1.4 Innovation / New Technology	Adoption of significant new technology that changes how the technology service is provided must be notified to the LBG Supplier Manager ahead of implementation, for example a move to a cloud service.
2.1.5 Skills and Expertise	Levels of IT resourcing and IT subject matter expertise for LBG hosted systems must be monitored to ensure continuity of development and operation of technology services.

2.2 BUILD, CHANGE AND ACQUISTION

2.2.1 Technical Design and Build	Technology services must be designed, developed, tested and implemented to meet LBG approved requirements.
2.2.2 IT Change Management	IT changes to production technology services must be risk and impact assessed, with all changes and required approvals managed through an IT Service Management tool. 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 IT 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 where there is potential to impact critical services. Back-out plans must be tested and proven to recover technology services and avoid consequential impacts.

2.3 AVAILABILITY, PERFORMANCE AND RECOVERY

2.3.1 Service Hosting Environments	Technology services that are critical to an LBG Critical Business Process, i.e. break the service chain, 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 is part of an LBG Critical Business Process it must be maintained in line with LBG IT resilience requirements and subject to ongoing review at a minimum annually and for any material changes.
2.3.3 Technology Currency	IT hardware and software 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 Recovery Proving / Assessment	IT disaster recovery capability of a technology service must be proven on a scheduled basis or following a material IT change to evidence that LBG Business Impact Assessment availability and integrity requirements can be met. New implementations must undertake DR proving (including LBG connectivity) within 4 weeks of service commencement. Proving 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 a secondary location IT disaster recovery RTO/RPO and proving frequency requirements must be detailed in the contract for provision of the technology service.
2.3.5 Failed Recovery Proving	Any failed disaster recovery proving and remediation action required must be notified to the LBG Supplier Manager or relevant Business contact. Recovery proving must be retested successfully within 3 months of the failure.
2.3.6 Service Incident and Problem Management	Recovery from technology service incidents must be timely to meet service level agreements and remain within LBG risk appetite for LBG Critical Business Processes and LBG Business Impact Assessment availability requirements. 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 LBG Supplier Manager any incidents for other clients that have the potential to also impact technology service provided to LBG.

2.4 OPERATION

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

2.5 SECURITY

For technology security requirements, refer to the Group Information & Cyber Security Policy.

.

2.6 Definitions

Technology Service(s)	Refers to the technology related elements of the service provided by the supplier, including IT systems, infrastructure, applications, networks, processes and people.
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

3.0 KEY CONTROLS		
Control Title	**Control Description**	**Frequency**
Technology solutions 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	Ad hoc

	functional test environment is reflective of the live environment or a justification for it not reflecting live is documented	
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, 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 management process is fully implemented	• A process for Incident Management is documented • All incidents are logged, prioritised and assigned to the relevant teams for timely response and investigation • Incidents 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 alerts managed and trend analysis performed	Annually Ad hoc
Proving programme for critical systems and core technology infrastructure 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	Annually

4.0 VERSION CONTROL
Any control failures or material differences between the requirements set out above and the supplier's own controls should be raised by the Supplier with the Group's Supplier Manager or relevant Business contact.

Version Number	Effective Date
1.0	30th November 2017
2.0	30th July 2018
3.0	1st January 2020
Next Planned Revision: January 2021	