LLOYDS
BANKING GROUP

# External Supplier Policies

June 2026

Version 1.0

# BEING A SUPPLIER TO LLOYDS BANKING GROUP

We're committed to ensuring that all our dealings with external suppliers are conducted in accordance with the principles of fair and ethical trading, from initial sourcing to ongoing supplier management, as well as in situations where we need to exit contracts.

We only work with suppliers who are committed to delivering the required level of performance and quality that our customers expect.

We expect our suppliers to take time to understand our business and look for ways to bring insight and enhancements.

By strengthening the way we do business, we can continue to generate the innovative products, services and solutions that our customers deserve.

## OUR POLICY REQUIREMENTS AND APPLICABILTY

Lloyds Banking Group's External Supplier Policies set out the expectations placed on all external suppliers we receive goods and services from and are aligned to the key areas of risk we face.

By understanding and meeting the requirements outlined in this document you will help us to ensure:

- Our services are resilient, and service disruption is prevented or limited.
- Good outcomes are consistently delivered to our customers.
- Regulatory expectations are met.

The applicability of each individual policy is based on the services provided. Suppliers are encouraged to review the applicability statement at the beginning of each section in addition to any pre-existing contractual obligations to determine which requirements apply.

## SUPPLY CHAIN DUE DILIGENCE EXPECTATIONS

We expect all suppliers to perform due diligence that is appropriate and proportionate to the requirements outlined in this document, prior to onboarding any sub-contractors, and on an ongoing basis.

Any issues identified should be resolved in line with our risk management expectations.

Lloyds Banking Group will perform proportionate ongoing monitoring, oversight and assurance of supplier activities to ensure compliance with all policy requirements.

## RISK MANAGEMENT EXPECTATIONS

In addition to the requirements set out in this document, we expect all suppliers to have a robust risk management framework in place to ensure:

| |
|---|
| Risks are appropriately identified, assessed and managed in a timely manner. |
| Controls are operated to sufficiently mitigate identified risks and events. |
| Events and incidents are reported to Lloyds Banking Group on a timely basis. |
| Periodic risk and control MI is complete, accurate and reported to Lloyds Banking Group within agreed timescales. |

### CODE OF SUPPLIER RESPONSIBILITY

We want our suppliers to share in our purpose and ensure that they operate in an ethical, sustainable, inclusive and accessible manner. We therefore expect all of our suppliers to practice our Code of Supplier Responsibility.

The code sets out the key social, ethical and environmental values and behaviours that we expect you to abide by.

## CONTACT

If you, as a supplier, are unclear how the requirements outlined in this document apply to you, please engage your Lloyds Banking Group Supplier Manager or usual contact.

# Contents

# 1. ANTI-BRIBERY RISK POLICY REQUIREMENTS

These requirements must be followed to manage the risk that a colleague or external supplier that acts on behalf of the Group, offers, requests or receives (whether accepted or not) a bribe as inducement for acts of dishonesty, illegal activity or breach of trust.

| Requirement | Description |
|---|---|
| Purpose | The purpose of this policy is to support the effective management of anti-bribery risk in relation to external suppliers providing services to, for, or on behalf of Lloyds Banking Group. It sets out the Group's expectations for preventing, identifying, escalating and responding to bribery risks, including the offer, promise, payment, request, receipt or acceptance of any bribe by an individual, supplier or associated party.<br><br>The policy is designed to help ensure a consistent, proportionate and effective approach to anti-bribery controls and to support compliance with applicable anti-bribery legislation and regulation in the UK and in any other jurisdiction in which the Group operates. The Group has no appetite for breaches of bribery legislation or regulation, including breaches arising from activities conducted by external suppliers or other parties acting on the Group's behalf. |
| Applicability | These policy requirements apply to external suppliers where it has been determined that the Anti-Bribery Risk Policy is applicable to the services they provide to, for, or on behalf of the Group. |
| Scope | This policy applies to bribery risks connected to external suppliers and associated parties involved in the delivery of products or services to, for, or on behalf of the Group. This includes risks arising from improper payments, offers, promises, requests or agreements to give or receive any advantage as an inducement to act improperly in the conduct of the Group's business, including anything dishonest, illegal or involving a breach of trust.<br><br>The policy supports compliance with relevant legal and regulatory requirements, including the Bribery Act 2010, Ministry of Justice guidance issued under section 9 of the Bribery Act 2010, the Proceeds of Crime Act 2002, applicable Financial Conduct Authority requirements and guidance, the US Foreign Corrupt Practices Act 1977, and any other jurisdictional legislation with extra-territorial application.<br><br>Where local legislative or regulatory requirements exceed the standards set out in this policy, the external supplier must comply with the higher standard. |
| Principle Prohibition | The Supplier, and anyone engaged by the Supplier to act for or on behalf of the Group, must not:<br><br>a) offer, promise, give, request, agree to receive or accept a bribe; or<br><br>b) do anything to circumvent controls in place to deter, prevent or detect bribery. |
| Prevention of Corruption | Corruption is defined as the abuse of entrusted power for private gain and is a term used to describe a wide range of financial misconduct.<br><br>The Group has zero appetite for acts of corruption committed by colleagues, customers or suppliers. Any incidents or potential incidents of corruption (by employees of the Supplier or any other persons who will perform services on behalf of the Group) must be reported in accordance with the reporting requirements of this and any related policies that deal with activities that fall under the definition of corruption.<br><br>Dealings with Public Officials may pose a greater corruption risk due to their position and status. Under section 6 of the Bribery Act 2010 it is a specific offence to bribe a foreign public official. Suppliers must, when dealing with any Public |

| | |
|---|---|
| | Official, ensure that appropriate steps are taken to minimise the bribery and corruption risks associated with relationships of this nature. |
| Required Procedures | The Supplier must ensure that in respect of the activities carried out for or on behalf of the Group, it operates policies and procedures (including controls, processes and operations) designed to manage the risk of bribery, which are:<br>• proportionate to the bribery risk (as identified through a risk assessment exercise).<br>• appropriate and relevant for the type of business.<br>• communicated to relevant parties (internal and external), including the Group.<br>• documented in a clear comprehensible manner and accessible to all relevant persons; and<br>• reviewed regularly to ensure they remain up-to-date and reflect current practice. |
| Top Level Commitment | Effective top-level commitment allows an organisation to drive an appropriate and effective anti-bribery culture. Suppliers may consider appointing a nominated individual(s) with technical expertise and professional credibility to be responsible for the management of anti-bribery risk in a similar manner to the structure utilised within the Group. |
| Threat & Risk Assessment | The supplier must undertake a regular anti-bribery risk assessment in order to identify and mitigate the bribery risks associated with the conduct of its business. |
| Due Diligence | The supplier must complete risk-based anti-bribery due diligence on persons (including individuals and incorporated or unincorporated bodies) who will perform services for or on behalf of the Group which is appropriate and relevant to such services. Further guidance on risk-based due diligence can be obtained from your supplier manager if required.<br>In determining whether a person is acting for or on behalf of the Group, the supplier must consider the nature of the activity being undertaken. As a minimum, an agent, subsidiary or any other person obtaining, retaining or conducting business on behalf of the Group must be subject to due diligence.<br>The supplier must, as part of their due diligence activities, identify all directors and perform appropriate additional checks to ascertain whether or not any of the directors are public officials and/or politically exposed persons (PEPs). Where the nature of the services provided and the involvement of public officials and/or PEPs leads to an increase in bribery risks, further guidance must be sought from your supplier manager. |
| Due Diligence for sub-contractors | The supplier must perform appropriate and proportionate due diligence on your sub-contractors before onboarding them and on an ongoing basis. |
| Due Diligence for employees | The supplier must assess the need for, and extent of, ongoing due diligence for persons engaged by it to identify and mitigate bribery risks. |
| Monitoring & Review | The supplier must ensure that arrangements are in place to monitor regularly the continued adequacy and effectiveness of processes, systems and controls in order to assess compliance with this document. This will include any assurance, oversight and/or audit reviews.<br>Where deficiencies are identified, suppliers must resolve them without delay, escalate to the Group where appropriate and monitor thereafter to identify and prevent any recurrence. |
| Charitable Donations | The supplier must not make any donations to charities for or on behalf of the Group. |

| | |
|---|---|
| Political Donations | The supplier must not make any political donations for or on behalf of the Group |
| Facilitation Payments | Facilitation payments are illegal under UK law. A facilitation payment is a payment which is made to expedite or secure the performance of a routine non-discretionary action, such as processing papers, issuing permits, and other actions by a person which they are already bound to perform.<br><br>Facilitation payments which relate in any way to the services provided to Lloyds Banking Group are prohibited. In exceptional circumstances of duress (only where there is a threat to life, limb or liberty) facilitation payments may have to be made. Where possible, prior approval from the Group must be obtained. In any event, all such facilitation payments must be reported to the Group immediately.<br><br>The supplier must ensure that:<br><br>• the risk of facilitation payments which relate in any way to the services provided to the Group being requested is included in their risk assessment.<br><br>• all requests for such facilitation payments are reported to the Group.<br><br>• suitable procedures to mitigate the risk are in place where there is a likelihood that facilitation payments will be requested (e.g. in certain jurisdictions). These procedures must include specific training for individuals who may have to manage such requests; and<br><br>• all those acting for or on behalf of the Group are aware of their responsibilities in respect of facilitation payments even where these are declined or refused. |
| Reporting | The supplier must ensure that all persons engaged by it are aware of routes to report instances of suspected bribery or attempted bribery.<br><br>To the extent permitted under applicable law, the supplier will, as soon as is reasonably practicable, notify the Group in the event that a person acting on its or the Group's behalf is suspected of bribery or corrupt practices.<br><br>The supplier will promptly notify the Group if the supplier, or any person engaged by it, is prosecuted, charged with or convicted of any bribery-related offence. |
| Record Keeping | The supplier must retain all records (electronic and paper, and including relevant training records) in line with the requirements found in the Group Data & Privacy Risk Policy |
| Training | The supplier must ensure that all employees complete anti-bribery training and awareness activities appropriate to both their individual roles and the level of bribery risk associated with the role.<br><br>The supplier must ensure all employees / contractors complete Anti-Bribery training no later than 8 weeks from the commencement of their employment and annually thereafter to understand how the requirements of relevant anti-bribery legislation and this Policy Summary affect their role and individual responsibilities.<br><br>Where employees are identified as working in roles considered high risk for bribery, role specific training must be considered to ensure that employees are aware as to the increased bribery risks and expected controls associated with their roles. |
| Management Information | External Suppliers must ensure that key anti bribery management information is produced and evidence is available by the Group Supplier Manager. This includes but not limited to:<br><br>• Training<br><br>• Charitable Donations<br><br>• Political Donations<br><br>• Facilitation Payments |

| | |
|---|---|
| | • Due Diligence Completeness<br>• High Risk Suppliers<br>The External Supplier must ensure that Governance arrangements are in place that ensure the escalation of MI and results of oversight and monitoring programme to the External Suppliers Senior Management and LBG (as agreed) allowing for the effective management of Bribery risks in a timely manner. |
| Non-Compliance | Any material 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.<br>The Supplier Manager will then discuss the non-compliance with the Accountable Executive for the relationship and local Risk team to agree way forward |

# 2. ANTI-MONEY LAUNDERING RISK POLICY REQUIREMENTS

These requirements must be followed to manage the risk that Group products or services are used for money laundering, terrorist financing, proliferation financing or facilitation of tax evasion. Legal requests for information relating to Economic Crime (or money laundering) served by law enforcement agencies or the Regulator must be appropriately responded to.

| Requirement | Description |
|---|---|
| Purpose | This Policy sets out the consistent requirements and parameters which must be followed to manage Economic Crime Risk within Board approved risk appetite and enable compliance with all applicable regulation, legislation and associated standards that the Group must adhere to.<br><br>The Group Economic Crime Prevention Risk Policy defines the minimum global requirements to support the management of economic crime related risks. These requirements have primarily been informed by UK regulation.<br><br>No one in the Group, or acting on its behalf, must frustrate or circumvent the intended purpose of this Risk Policy.<br><br>This summary sets out how the Economic Crime Prevention Policy (Anti-Money Laundering) requirements apply to External Suppliers. |
| Applicability | The Economic Crime Prevention Policy is a mandatory requirement for all businesses, divisions and legal entities within the Group and applies to all colleagues (temporary and permanent) in all jurisdictions in which the Group operates. The Policy clearly articulates a set of minimum standards and requirements that meet and often exceed UK regulatory and legislative obligations and industry guidance such as that provided by the Joint Money Laundering Steering Group (JMLSG).<br><br>In jurisdictions where the local legislative and regulatory requirements exceed the requirements set out in this document, the external supplier must comply with any higher standards. |
| Scope | An external party supplying services to the Group or performing services on the Group's behalf will be expected to comply with the Group's Economic Crime Prevention Policy where those services form part of the Group's regulated activities.<br><br>In all other circumstances, this Policy is not applicable to external suppliers of goods or services to the Group.<br><br>Typical circumstances that will result in the AML/CTF requirements of the Economic Crime Prevention Policy being applicable include the following services:<br><br>• On-boarding or introducing customers;<br>• Processing customer transactions;<br>• Providing the Group's financial products to customers; and<br>• Providing risk, compliance or audit services to the Group.<br><br>Typical circumstances that will not result in the AML/CTF requirements of the Economic Crime Prevention Policy being applicable include:<br><br>• Providing goods to the Group;<br>• Performing services unrelated to the Group's regulated activities (e.g. security, transport, catering, printing, etc.); and |

| | |
|---|---|
| | • Conducting activities outside the scope of Regulation 8 of the UK Money Laundering, Counter Terrorist Financing (Amendment) (EU Exit) Regulations 2020(or equivalent) |
| Due Diligence | Perform appropriate and proportionate due diligence on your sub-contractors before onboarding them and on an ongoing basis. |
| Compliance with Money Laundering Regulations | The external supplier must comply with any Legal or Regulatory obligations to which they are subject in their own right, for example, by virtue of their falling within the scope of Regulation 8 of the UK Money Laundering, Counter Terrorist Financing (Amendment) (EU Exit) Regulations 2020 (or equivalent).<br>The external supplier must not engage in any conduct that results in it, or another party:<br>• concealing, disguising, converting or transferring criminal property or terrorist funds.<br>• entering into or becoming concerned in an arrangement that facilitates the acquisition, retention, use or control of criminal property terrorist funds; or funds intended for the use of proliferation of weapons of mass destruction.<br>• acquiring, using or possessing criminal property; terrorist funds; or funds intended for the use of proliferation of weapons of mass destruction; or facilitating Tax Evasion. |
| Compliance with Money Laundering Regulations – LBG maintaining accountability | Where the external supplier is supplying a service to Lloyds Banking Group or performing a service on behalf of the Group that forms part of the Group's regulated activities and for which Lloyds Banking Group retains accountability, the Group will define for the external supplier the specific requirements of the Economic Crime Prevention Policy relevant to that service. This may include some or all of the following:<br>Assessment of money laundering, terrorist financing and proliferation financing risk.<br>Customer Due Diligence / Ongoing Customer Due Diligence (including forwarding CDD material upon request);<br>• Transaction Monitoring.<br>• Suspicious Activity Reporting.<br>• Responding to Court Orders.<br>• Provision of Management Information.<br>• Staff Training; and<br>• Record Keeping.<br>In all cases, Lloyds Banking Group will perform ongoing monitoring, oversight and assurance of the external supplier's activities to ensure compliance with the Economic Crime Prevention Policy. |
| Management Information | External Suppliers must ensure that MI is produced that includes details on the levels of compliance in relation to:<br>• Training;<br>• Due Diligence completeness (CDD/EDD);<br>• ODD;<br>• PEP Screening activities;<br>• SAR escalation activities; |

| | |
|---|---|
| | • Record keeping.<br>• MI must also identify where remedial action is required.<br>The External Supplier must ensure that Governance arrangements are in place that ensure the escalation of MI and results of oversight and monitoring programme to the Third Parties Senior Management and LBG (as agreed) allowing for the effective management of ML/TF risks in a timely manner. |
| Training | The external supplier must ensure all employees / contractors complete Anti Money Laundering, Counter Terrorist Finance & Counter Proliferation Finance training no later than 8 weeks from the commencement of their employment and annually thereafter to understand how the requirements of relevant anti money laundering legislation and this Policy Summary affect their role and individual responsibilities.<br>Where employees are identified as working in roles considered high risk for Money Laundering, role specific training must be considered to ensure that employees are aware as to the increased Money Laundering risks associated with their roles. |
| Non-Compliance | Any material differences between the requirements set out above and the external supplier's own controls should be raised by the Supplier with Lloyds Banking Group's Supplier Manager.<br>The Supplier Manager will then discuss the non-compliance with the Accountable Executive for the relationship and local Risk team to agree way forward |

# 3. BUSINESS CONTINUITY POLICY REQUIREMENTS

The risks associated with the failure to identify the services and processes that should be protected from unavailability; that we do not plan for our response during unavailability; or that plans fail at the point at which we invoke them.

| Requirement | Description |
|---|---|
| Purpose | These requirements must be followed to manage the risks associated with the failure to identify the services and processes that should be protected from unavailability; that we do not plan for our response during unavailability; or that plans fail at the point at which we invoke them.<br>The requirements set out below are our minimum Business Continuity requirements designed to protect:<br>• The delivery of our Important Business Services (these are services, which if disrupted could cause customer intolerable harm, or a risk to LBG's safety and soundness; the financial stability of the UK, or to policyholder protection); and<br>• The delivery of our Priority Processes (these are processes which if disrupted could lead to a Severe or Material impact for LBG). |
| Applicability | LBG will determine and communicate the applicable classification of services being provided by an External Supplier, including where these are critical to an Important Business Service, or Priority Process.<br>Business Continuity requirements are applied proportionately based on this classification. LBG may also choose to extend these requirements to other services at their discretion.<br>For services provided that are critical to our Important Business Services and Priority Processes, LBG will undertake assurance testing of requirements. |
| Scope | This document sets out the minimum Business Continuity requirements that apply to External Suppliers, to protect the services being provided to Lloyds Banking Group. These are determined by service criticality and may include: Asset Mapping; Business Continuity Planning & Testing; Scenario Testing; Incident Management and Vulnerability Remediation. |
| **REQUIREMENTS FOR THE PROVISION OF SERVICES CRITICAL TO AN IMPORTANT BUSINESS SERVICE** | |
| Mapping of Assets (Frequency: Annual) | Map all key assets (Technology, Data, People, Premises, Suppliers) required to deliver the service. As a minimum, mapping will:<br>• Enable the identification of vulnerabilities that could materially affect the availability of the service(s) being provided to LBG.<br>• Enable you to test your ability to remain within tolerances agreed with you, for each of our Important Business Services.<br>• Where you have sub-contracting arrangements in place, these nth parties shall be identified and mapped by you. |
| Business Continuity Planning (Frequency: Annual) | Have Business Continuity Plans in place for all key assets and undertake annual proving of plans for the provision of all services critical to an Important Business Service. Where testing shows that there are weaknesses in your plans that impact performance against tolerances agreed with you, corrective action shall be taken, and your plans updated and retested, within an agreed suitable timeframe. |
| LBG-led Scenario Testing | For the provision of services critical to an Important Business Service, you may be invited to take part in periodic LBG-led collaborative scenario testing activity to assess ability to remain within Impact Tolerances (ITOLs). Supporting evidence |

| | |
|---|---|
| (Frequency: Periodic) | shall be required to validate your response and recovery actions from the test, including timescales referenced. Evidence should be as close to live as possible.<br><br>The approach to collaborative testing is designed to identify vulnerabilities. Where recovery within ITOL is not possible, agreed response actions will need to be remediated by you. |
| Supplier-led Scenario Testing | For the provision of services critical to an Important Business Service, you are required to undertake your own scenario testing to assess your ability to remain within tolerances agreed with you. Test outcomes and vulnerability identification shall be shared with us.<br><br>For the provision of services critical to an Important Business Service, ensure that the necessary corrective actions are taken to address vulnerabilities identified to ensure you can remain within tolerances agreed with you.<br><br>Where vulnerabilities cannot be remediated, you are required to implement interim mitigating actions pending longer-term remediation. |
| Vulnerability Remediation | For the provision of services critical to an Important Business Service, ensure that the necessary corrective actions are taken to address vulnerabilities identified to ensure you can remain within tolerances agreed with you.<br><br>Where vulnerabilities cannot be remediated, you are required to implement interim mitigating actions pending longer-term remediation. |
| Incident Management | Respond to incidents with timely and clear communication regarding the provision of services being provided to LBG. LBG may request additional detail depending on the impact of the incident to LBG.<br><br>Share relevant Post-Incident Reports with LBG, including Root Cause Analysis and Lessons Learned, as soon as reasonably practicable. |
| Self-Assessment (Frequency: Annual) | An annual Self-Assessment is required for the provision of services that are critical to an Important Business Service, setting out how you have met the related requirements above. |
| **REQUIREMENTS FOR THE PROVISION OF SERVICES CRITICAL TO A PRIORITY PROCESS** | |
| Identify denials | Identify all denials (Denials include Technology, Data, People, Premises, Suppliers) required to deliver the service(s) being provided to LBG. Where you have sub-contracting arrangements in place, these nth parties shall be identified by you to inform Business Continuity Planning. |
| Business Continuity Planning (Frequency: 12 or 24 months; this will be agreed with you) | Have Business Continuity Plans in place for all key denials (please see above) and undertake risk-based proving of plans for the provision of all services. A minimum testing frequency of either 12 or 24 months will be agreed with you, depending on criticality of LBG process.<br><br>Where testing shows that there are weaknesses in your plans that impact performance against tolerances agreed with you, corrective action shall be taken, and your plan updated and retested, within an agreed suitable timeframe. |
| Incident Management | Respond to incidents with timely and clear communication regarding the provision of services being provided to LBG. LBG may request additional detail depending on the impact of the incident to LBG.<br><br>Share relevant Post-Incident Reports with LBG, including Root Cause Analysis and Lessons Learned, as soon as reasonably practicable. |
| Management Information | Management Information will be requested on a proportionate and agreed basis, to demonstrate compliance with these requirements. |
| **MINIMUM REQUIREMENTS FOR ALL OTHER SERVICES** | |

| | |
|---|---|
| Business Continuity Planning<br><br>(Frequency: 24 months) | As a minimum we expect you to have Business Continuity Plans in place to ensure you can continue to provide an agreed level of service to us.<br><br>You shall undertake risk-based proving of plans, and a minimum testing frequency of at least 24 months will be agreed with you.<br><br>We will require you to attest to us that you have plans in place which have been tested and proven and share output on request.<br><br>Where available, we will take ISO 22301 certification into account as supporting evidence. |

# 4. CHANGE EXECUTION RISK POLICY REQUIREMENTS

The risk of failure to effectively prioritise, execute, implement and adopt Change across the Group to achieve organisational objectives and / or mitigate adverse impacts on customers and colleagues arising from Change.

| Requirement | Description |
|---|---|
| Purpose | Defines for in scope External suppliers the expected change management requirements which address the risk of failure of an external supplier to effectively prioritise, execute, implement and adopt change to achieve agreed objectives and / or mitigate adverse impacts on customers and colleagues arising from that change. |
| Applicability | Suppliers who meet this applicability must be able to meet the below requirements through application of their own Change methodology and its associated processes.<br>Suppliers must ensure:<br>• All changes delivered supporting Group services, including downstream supplier relationships, comply with contractual agreements and schedules of work.<br>• Changes are delivered to jurisdictional industry minimum standards and are compliant with local, international, statutory, legislative, contractual and regulatory requirements. |
| Scope | These requirements are applicable to External suppliers who provide goods and services to the Group and / or its customers and deliver changes to their own IT systems and / or processes. |
| Planning | The Supplier ensures plans are in place to confirm the change will be delivered in agreed timelines. |
| Delivery Risk Management | The Supplier performs monitoring activity to ensure impacts of material delivery risks on commitments are understood and appropriate action plans are in place to mitigate them, with material risks escalated to LBG promptly. |
| Dependencies | The Supplier performs monitoring activity to ensure impacts of critical dependencies on commitments are understood and appropriate action plans are in place to mitigate them, with any progress issues escalated to LBG promptly |
| Progress | The Supplier performs monitoring activity to ensure progress and pace of delivery is in line with committed timescales. |
| Design | The Supplier performs validation activity to ensure that the requirements and design are understood, documented and traceable to ensure the defined scope will deliver the intended outcome. |
| Change Impacts | The Supplier performs validation activity to ensure impacts of the change to LBG have been identified and required actions/engagements have been completed. |
| Testing | The Supplier performs documented validation activity to ensure the functional and non-functional testing completed is sufficient and meets expected industry standards and proves the design, and the change can be deployed to the level of availability and capacity required prior to the change being deployed. |
| Implementation Readiness | The Supplier performs documented validation activity to ensure, ahead of implementation, approval from all impacted business areas, including LBG, of delivery readiness has been obtained. |

# 5. CLIENT ASSETS RISK POLICY REQUIREMENTS

The risk arising from failure to follow (specific) rules, regulations and laws (including codes of practice) that apply to all stages of the customer and product journeys and managing our relationship with our regulators.

| Requirement | Description |
|---|---|
| Purpose | This Policy sets out the requirements that suppliers must comply with when providing services involving Client Assets, to support the protection of client money and custody assets and compliance with applicable legal and regulatory requirements. |
| Applicability | This Policy applies to suppliers and other third parties that receive, hold, process, manage, administer, or otherwise support services involving Client Assets on behalf of the Group. |
| Scope | This Policy covers all supplier activities that could impact the safeguarding, identification, segregation, record keeping, reconciliation, reporting or return of Client Assets, including client money and custody assets. |
| Compliance with CASS Regulations | Undertake all activity in accordance with the CASS regulations |
| Adherence to CASS Service Schedules and Metrics | Adhere to all CASS Service Schedules and metrics, including but not restricted to:<br>• Record, report and manage CASS breaches to closure with appropriate mitigating actions.<br>• Maintain a CASS Control Framework required by the Financial Reporting Council's CASS Assurance Standard.<br>• Support Internal and External CASS Audit Processes.<br>• Maintain records required in the CASS Resolution Pack in accordance with CASS 10.<br>• Provide accurate data to support timely submission of the monthly Client Money and Asset Return.<br>• Provide regular CASS governance reporting |

# 6. COLLEAGUE CONDUCT RISK POLICY REQUIREMENTS

The risk that poor colleague behaviours adversely impact customers, colleagues or business operations.

| Requirement | Description |
|---|---|
| Purpose | Strong personal conduct underpins safe, compliant and effective service delivery and is essential to managing regulatory, operational and reputational risk.<br><br>These requirements set out the standards external suppliers must meet to ensure that their behaviour, and that of the individuals they assign to the Group, does not adversely impact customers, colleagues, or business operations. Failure to meet these standards may result in customer or reputational harm to the Group and may lead to contract termination. |
| Applicability | The Personal Behaviours section applies to all external suppliers.<br><br>All other sections of this policy apply to external suppliers who assign individuals to work for or on behalf of the Group.<br><br>The regulated roles section applies only to external suppliers who assign individuals to regulated roles, i.e. those in scope of the Senior Managers and Certification Regime (SMCR). |
| Scope | External suppliers operating outside the UK must comply with all UK legislative, regulatory and policy requirements set out in this document, as a minimum standard, in addition to any applicable local legal or regulatory requirements.<br><br>Where local legal or regulatory requirements exceed the UK requirements set out in this document, external suppliers must comply with the higher standard.<br><br>Where local legal or regulatory requirements are less stringent than the UK requirements set out in this document, external suppliers must continue to comply with the UK requirements in full.<br><br>Where external suppliers are unable to meet a requirement, they must notify their Supplier Manager without delay. The Supplier Manager must engage the Policy Owner to agree an alternative compliant approach. |
| Personal Behaviours | In addition to the requirements set out in the Code of Supplier Responsibility, all external suppliers must:<br><br>• Act professionally, with integrity, and treat others with respect.<br>• Take personal responsibility for their own behaviour and actions.<br>• Avoid dishonesty or any act that could harm the reputation of an individual or the Group.<br>• Communicate respectfully and professionally. External suppliers must not engage in behaviour that is abusive, obscene, offensive, discriminatory, threatening or defamatory, including offensive comments, jokes, crude remarks, bullying intimidation, threats or any other context that could cause harm or offense.<br>• Not engage in reckless behaviour or actions that create unacceptable risk.<br>• Act respectfully, free from discrimination, harassment, sexual harassment, violence, bullying, victimisation, or retaliation.<br>• Avoid inappropriate behaviour, including unwelcome touching, sexual advances, or rude gestures. |

| | |
|---|---|
| | • Report any concerns that could damage the Group's reputation to the Supplier Manager, regardless of whether they are directly involved, to enable timely investigation and appropriate action by the Group. |
| Policy Adherence | External suppliers must ensure assigned individuals:<br>• Are contractually required to comply with all Group policies and processes relevant to the service they provide. |
| Roles and Responsibilities | External suppliers must:<br>• Understand the specific role requirements, including all conduct, regulatory, operational, and customer-related expectations.<br>• Clearly define, agree, and document the roles and responsibilities of every individual provided to the Group, specifying tasks, services, and expected standards to support clear accountability and reduce the risk of poor conduct arising from unclear roles or inappropriate delegation. |
| Competence, Capability and Capacity | External suppliers must:<br>• Ensure, prior to onboarding and on an ongoing basis, that conduct concerns or behavioural incidents (including patterns of behaviour) are considered when assessing whether an individual is suitable, competent and capable to perform their role on behalf of the Group, to protect customers, colleagues and the Group from conduct, regulatory or reputational harm. |
| Policy Standards and Communication | External suppliers must:<br>• Maintain a legally compliant conduct policy, with full version control, that sets clear standards for integrity, behaviour, compliance and competence. It must be reviewed and communicated regularly, retaining evidence of communication and review. All updates to the policy, must be shared promptly with appointed individuals.<br>• The policy must be reviewed and approved by a suitably qualified individual (e.g. HR or in house legal) or an external legal adviser. The supplier must be able to attest that this review has taken place.<br>Where waivers or exceptions are approved, the rationale and approval must be documented. |
| Conduct Rules | External suppliers must:<br>• Ensure assigned individuals adhere to regulatory Conduct Rules.<br>• Maintain a conduct rule breach policy or procedure that includes version control and clearly defines how conduct breaches are identified, assessed, managed, and escalated.<br>• Operate a documented process for managing conduct breaches, including prompt investigation, documented decision-making, and consistent consequence management.<br>• Track, record, and evidence breach outcomes, including cases where misconduct may breach regulatory rules or standards, and report these to their supplier manager and the Group in line with agreed timelines. |
| Managing Misconduct, and Performance | External suppliers must:<br>• Maintain a disciplinary process to manage misconduct and ensure material or reportable conduct issues are escalated to the Supplier Manager immediately upon identification.<br>• Identify, manage and remediate misconduct, performance or capability issues and escalate relevant issues to the Group without delay. |

| | |
|---|---|
| | • Ensure assigned individuals feel able to raise concerns about misconduct or inappropriate behaviour safely and without retaliation, through their own channels and, where applicable, the Group's Speak Up arrangements. |
| Mandatory Training<br><br>(Frequency requirement) | External suppliers must:<br>• Ensure all assigned individuals complete the supplier's own conduct or personal integrity training. This training must be version controlled and cover integrity, conduct, competence standards, regulatory obligations, consequences of misconduct and where to access support.<br>• It must include a defined passing requirement and be delivered within 8 weeks of induction and annually thereafter.<br>• Ensure all assigned individuals with access to LBG systems, complete mandatory and role specific training required by the Group, within the required timescales. This includes:<br>  ○ Conduct Rules Training (completed within the first four weeks of being assigned and annually thereafter)<br>  ○ Completion of all Training & Competence (T&C) requirements for roles in scope of a T&C scheme.<br>External suppliers must monitor, record and evidence all training completion (including completion date and passing rate) and provide this information to the Group upon request and within agreed timescales. |
| Supplier Oversight and Assurance | Where assigned individuals work under direct Group supervision:<br>• External suppliers remain responsible for ensuring standards are met, providing supporting information and evidence when required. Conduct, performance or competence issues must be escalated to the Group promptly.<br>Where assigned individuals are not under direct Group supervision:<br>• External suppliers must operate appropriate supervision, monitoring, quality assurance and conduct oversight, providing evidence to the Group on request. |
| Regulated Roles (where applicable)<br><br>(Regulatory Training - Frequency requirement) | In addition to the requirements listed above, when external suppliers are assigning individuals into a regulated role (those in scope of a Financial Conduct Authority (FCA)/Prudential Regulation Authority (PRA) regulatory accountability regime, including the Senior Managers and Certification Regime) they must:<br>• Maintain, monitor and keep an up to date a register of all assigned individuals performing regulated roles, and provide this to the Group upon request.<br>• Understand all regulatory requirements relevant to the role and cooperate fully with any regulatory requests or enquiries arising during the performance of their own or their assigned individuals' duties.<br>• Ensure delegation of tasks or responsibilities for regulated roles is made to appropriately skilled, qualified, and capable individuals, and that all delegations are clearly documented and subject to ongoing oversight to meet the Group's regulatory standards.<br>• Maintain processes to ensure assigned individuals provide sufficient, accurate information to enable the Group's assessment of Fitness and Propriety (in accordance with SMCR requirements).<br>• Maintain processes to ensure assigned individuals provide accurate and timely personal integrity disclosures. This includes assessment, ongoing monitoring and prompt escalation to the Group.<br>• Make assigned individuals aware they will be subject to the Group's monitoring and assessment processes and must comply with the Group's ongoing screening requirements, due to their role presenting increased risk |

| | |
|---|---|
| | and being subject to enhanced regulatory scrutiny. Expectations and requirements for vetting are included within the People Risk Policy chapter.<br>• Ensure relevant assigned individuals understand the additional Conduct Rules for Senior Manager Function holders (SMFs).<br>• Engage proactively and appropriately with the Group to ensure that regulatory references issued by the Group are factual, accurate and fair, enabling the Group to meet its regulatory obligations.<br>• Ensure the recruitment process obtains and appropriately acts on regulated references covering the past six years.<br>Additionally:<br>• Conduct breaches that fall under the FCA/PRA conduct regimes must be managed and notified to regulators by the Group. External suppliers must provide supporting information to ensure the Group's compliance with the regime.<br>• If an assigned individual is alleged to have committed misconduct, external suppliers must provide the Group with all information required to support its own investigation and enable the Group to report any misconduct findings to the regulator, regardless of any investigation or disciplinary action taken by the supplier.<br>• External suppliers must ensure assigned individuals complete all relevant regulatory training. For external suppliers with access to LBG systems, this includes:<br>o Certification Function Holders – must complete the "Senior Managers and Certification Regime – Certified Colleagues" training when first certified, and annually thereafter.<br>o Senior Manager Function (SMF) holders and Notified Non-Executive Directors (NEDs) – must receive an SMCR briefing delivered by the Central Compliance team and provide an attestation of completion when first approved.<br>• External suppliers must provide management information on all the above requirements when asked to do so, within agreed timelines. This includes evidencing the satisfactory reporting and escalation of any colleague conduct risks, which may impact the provision of services to the Group or result in regulatory interest/censure. |

# 7. CONFLICTS OF INTERESTS POLICY REQUIREMENTS

The Risk that conflicts of interest are not managed in situations where individuals or businesses (including colleagues and representatives) have competing professional or personal interest, obligations, or motivations with respect to customers, clients, suppliers (or third parties).

| Requirement | Description |
|---|---|
| Purpose | This policy sets out the requirements which must be followed to manage Conflicts of Interest Risk. A conflict of interest arises when an individual's or organisation's personal, financial, or professional interests - actual, potential, or perceived - interfere, or appear to interfere, with their duty to act in the best interests of another party, such as a client, customer, colleague, supplier or third party. |
| Applicability | The Conflicts of Interest policy applies to external suppliers of Lloyds Banking Group ('the Group'), to the extent that they are involved in regulated activities relating to the Group's customers.<br>If the external supplier is not involved in regulated activities relating to the Group's customers, it is considered out of scope of the policy. |
| Scope | A conflict can arise from a current relationship or be present due to a past personal or professional relationship. Conflicts can arise from either personal or corporate situations.<br>Personal Conflicts are matters arising from employees as individuals. A corporate conflict occurs when a decision made or taken on behalf of a subgroup or business unit could conflict with the interests of another part of the business, customer(s) / clients(s) or the market. |
| Identifying, recording and management of conflicts of interest | Such external suppliers must ensure that they have appropriate and effective arrangements in place, that staff are aware of to ensure Conflicts of Interest are identified, disclosed, managed and recorded. Those arrangements should be reviewed annually by an appropriately senior owner and be available to the Group upon request. |

# 8. CUSTOMER CONDUCT RISK POLICY REQUIREMENTS

Customer Conduct: The risk of Group not providing good customer outcomes through our actions and behaviours

| Requirement | Description |
|---|---|
| Purpose | The Customer Conduct Risk Policy sets out the consistent requirements and parameters which must be followed to manage Customer Conduct Risk within the LBG's risk appetite and enable compliance with all applicable regulation, legislation and associated standards that the Group must adhere to. This summary sets out how the requirements in the Customer Conduct Policy apply to external suppliers. |
| Applicability | This Policy is mandatory and applies to all external suppliers, including third party Manufacturers, Distributors, Introducers, Intermediaries and Joint Ventures, that can impact customer outcomes. |
| Scope | This Risk Policy sets the Group's customer conduct obligations to all external suppliers who are involved in the product distribution chain, or in relation to the delivery of customer service and support, and communication with customers. These requirements are to ensure good outcomes, mitigate foreseeable risks and customer harm, meet regulatory obligations, and operate within the Group's risk appetite. |
| Policies & Procedures | External suppliers must have documented policies and procedures which set out their customer treatment processes including good outcomes for customers, effective Complaint Handling, managing Customer Vulnerability and Customers in Financial Difficulty. These must be reviewed at least annually. |
| Monitoring Customer Outcomes | External suppliers must collate and share relevant Customer Outcomes MI as agreed, and where relevant to the role undertaken by the supplier and required for LBG to monitor end-to-end customer outcomes (including segmentation that enables vulnerable customer cohorts to be monitored and compared to other cohorts). In addition, testing must be performed across key processes to confirm the process is working as planned, to ensure applicable regulation and legislation has been complied with, and to ensure customers are receiving good outcomes (and provide relevant insight to the supplier and LBG). Where risk of harm is identified, steps should be taken by the supplier to mitigate or remove the risk of harm to customers. |
| Customer Vulnerability & Financial Difficulty | External suppliers must have processes in place that enable identification and recording of vulnerability (including financial difficulty) using information reasonably available, including customer disclosure. Ensure reasonable adjustments or alternative routes are available, where practicable, so that customers with vulnerabilities can achieve equivalent outcomes to other customers. A vulnerable customer is someone who, due to their personal circumstances or characteristics, may be at increased risk of harm. Vulnerability may be permanent, temporary or situational. |
| Complaint Handling | Ensure that all customer complaints managed by external suppliers are identified, recorded, investigated, and resolved fairly, in accordance with regulatory requirements, including where applicable FCA Dispute Resolution (DISP) requirements. There must be appropriate processes in place to conduct Root Cause Analysis (RCA) to help both the Supplier and Lloyds Banking Group to understand the reasons for a complaint, and to take appropriate steps. |
| Communications | Ensure that all communications, sent by external suppliers to LBG customers or on behalf of LBG, must support good outcomes by providing information that equips customers to make effective, timely and properly informed decisions (i.e. they must be clear, fair and not misleading; meeting the information needs of customers; likely to be understood by the intended audience; accessible, balanced, accurate, timely and lawfully delivered in line with all applicable legal |

| | |
|---|---|
| | and regulatory obligations). Suppliers must provide relevant information in a timely manner to Lloyds Banking Group (and where applicable other parties in the distribution chain) when reasonably requested, and proactively where reasonably required to enable accurate and timely communications to customers. |
| Colleague Training | Ensure all external supplier colleagues must receive appropriate training to have the skills and knowledge necessary to ensure that good outcomes are delivered to customers (e.g. complaint handling, customer vulnerability and delivering good customer outcomes). Suppliers must ensure that controls are in place to verify completion and effectiveness of training within their areas of responsibility. |

# 9. CYBER & INFORMATION SECURITY RISK POLICY REQUIREMENTS (INCLUDING PHYSICAL DATA SECURITY)

The risk of information theft, disclosure, manipulation, destruction, or loss of access through a malicious or non-malicious actors' exploitation of IT assets, people, or premises.

| Requirement | Description |
|---|---|
| Purpose | This Risk Policy sets out the consistent requirements and parameters which must be followed to manage Cyber and Information Security (including physical data security) Risk within Lloyds Banking Group's approved risk appetite and enable compliance with all applicable regulation, legislation and associated standards that the Group must adhere to. Every External Supplier must know the Risk Policies that are relevant to their service and understand how to comply with these.<br><br>This Risk Policy defines the requirements that all External Suppliers and third parties who access, process or store our customer, business and colleague information, and IT systems that process this information, must use to inform how they do so in a safe and secure manner.<br><br>The Third-Party Supplier Security Schedule supporting this Risk Policy define how requirements should be implemented and should be read alongside this Risk Policy. Not adhering to the requirements and guardrails is likely to inhibit the ability for the Group to operate and transform to meet its strategic outcomes safely and at pace. |
| Applicability | The requirements documented within this Risk Policy are applicable to all External Suppliers. |
| Scope | The scope of the Cyber and Information Security (including physical data security) Risk Policy includes all information and technology assets and personnel within the External Supplier, and their information and technology supply chain, including:<br><br>• Digital information covering both structured data (e.g. databases), and unstructured data and information (e.g. email and reports), and physical information (e.g. printed material).<br><br>• Software and applications/workloads the External Supplier write (including End User Developed Applications (EUDAs)), acquires (e.g. third-party software as a service), and maintains e.g. code, application programming interfaces (APIs), databases, and batch processing.<br><br>• Hardware and virtual/physical infrastructure the External Supplier builds, configures, and maintains to host applications e.g. compute, storage and networking, and branch devices. This includes on premise hosting environments and cloud landing zones (production and non-production).<br><br>• Utilities and tools the External Supplier use to manage its applications/workloads and infrastructure services e.g. code repositories and development pipelines, asset and configuration management tools, and performance management tools.<br><br>• Technology vendors and third-party services the External Supplier consumes (including those mentioned above e.g. Software as a Service).<br><br>• The physical facilities that protect information and technology assets. |
| Information Security Management System | IT assets (physical and virtual) are accurately inventoried, have A security strategy is published, and associated security frameworks provisioned, to manage security risks and controls and maintain the effectiveness of an Information Security Management System (ISMS). |

| | |
|---|---|
| | Standards and patterns supporting security risk management are created and maintained to guide design and align with risk appetite |
| Security Improvements | Security management processes, procedures and activities are continuously improved.<br>Improvements are identified, assessed and implemented according to priority and evaluated for effectiveness. |
| Asset Inventory & Ownership | IT assets (physical and virtual) are accurately inventoried, have ownership assigned, and are managed and maintained throughout their lifecycle for optimal utilisation, support recovery in the event of an incident, cost-effectiveness, and compliance with regulatory and/or legal requirements. |
| Information Classification & Protection | Group information is assigned an owner, is classified based on its level of confidentiality and is protected throughout its lifecycle to prevent against theft, leakage, tampering, unauthorised or loss of access to information. |
| Acceptable Usage | External Supplier colleagues handling Group data adhere to a set of Acceptable Usage Responsibilities |
| Information Management Integrity | Systems and information are monitored to identify unauthorised, anomalous, or suspicious change to prevent the manipulation of information. |
| Information Management Data Leak Management | Endpoint devices (e.g. laptop, printer etc), servers, and networks (inc. cloud services) that process, store or transmit sensitive information have data leak management mechanisms applied to prevent and detect the unauthorised exfiltration of information. |
| Information Management Remote Locations | Group information stored or utilised in remote locations where there is limited physical security (e.g. home and international working) are subject to risk assessment and enhanced control to prevent theft, leakage, or unauthorised access to sensitive information. |
| Cryptography & Secrets Management | Cryptographic and Secret Management solutions (e.g. data encryption, digital signatures and certificates, authentication secrets, etc.) and processes, are established and maintained throughout their lifecycle to protect cryptographic material, information and systems from unauthorised access or modification. |
| Access Control: Identity Management | System accounts (human and non-human) are inventoried and associated with an approved identity to prevent invalid or unapproved identities being granted access to Group systems. |
| Access Control Authentication & Authorisation Management | System account entitlements are limited to what the account needs for its role or function, and access is granted after being positively authenticated, to prevent unauthorised or toxic combinations of system access. |
| Access Control Privileged Access Management | Privileged entitlements are limited, and usage is protected to prevent entitlement misuse, modification without permission, or abuse. |
| Access Control Access Governance | System accounts and entitlements are subject to periodic and trigger-based review (e.g. staff moving within or leaving) to prevent excessive and unrestricted access to Group systems. |
| Secure IT Development and Change Management | Software is subject to a Software Development Life Cycle (SDLC) process that assesses, tests, and approves the release of software design and deployment to prevent the introduction of material defects, vulnerabilities, and security events while maintaining service reliability. |

| | |
|---|---|
| Design and Build Assurance | Proposed security designs are reviewed for compliance with security architecture, patterns and standards, with recommendations made on how to improve security posture.<br>Testing validates that changes to IT assets have been built in accordance with the security-approved design |
| Network and Infrastructure Threat Detection: Host Systems | Systems (hosts) have threat detection and prevention capabilities deployed to detect, contain, and/or remove anomalous or suspicious activity (e.g. malicious software, modification of critical files and configurations etc.), preventing and limiting the impact of an intrusion. |
| Network and Infrastructure Threat Detection: Networks | Networks and gateways have threat detection and prevention capabilities deployed to detect, contain, and/or remove anomalous or suspicious activity (e.g. malicious traffic or unusual network traffic patterns etc.), preventing and limiting the impact of an intrusion. |
| Network and Infrastructure Boundary Restrictions on Network Traffic | Network traffic flowing across a boundary (physical or virtual) connecting assets of varying trust levels is defined, managed, and/or denied, preventing unauthorised access, data movement, or the introduction of malicious software. |
| Network and Infrastructure Enhanced Restrictions on Asset Communication | Applications, infrastructure, information, and supporting services are risk-assessed and where appropriate, have enhanced restrictions to limit and control communication between assets within the same, and across different environment boundaries, to protect information from being accessed, leaked, or modified. |
| Software Hardening | Software is hardened through adjustments to configuration to prevent exploitation, unauthorised disclosure, or exfiltration of information. |
| Physical and Virtual Infrastructure and Device Hardening | Physical and virtual infrastructure and devices (e.g. laptops, mobile phones, printers, physical servers, virtual machines, logical partitions etc.) are hardened through adjustments to configuration to prevent exploitation, unauthorised disclosure, or exfiltration of information. |
| Threat Intelligence | Security threat intelligence is identified, analysed, and disseminated to support the management of security threats (via downstream controls), that reduce the risk of security related attacks. |
| Security Testing | IT assets across all production environments are security tested proportionate to their threat exposure, to identify technical vulnerabilities, including security misconfigurations, enabling effective prioritisation and remediation in line with risk exposure. |
| Event Detection | Relevant security events are logged, monitored, and analysed to detect anomalous or malicious behaviour in near real-time, support incident response in limiting impact, and aid forensic investigations. |
| Incident Response | Security incidents are identified, investigated, contained, and reviewed for root cause to manage impacts and support timely restoration of services. |
| Cyber & Forensic Investigation | IT assets have capabilities deployed to enable forensic investigation and reconstruction of events that led to a security incident, and support in-progress and post incident investigation, to limit and recover from impacts. |
| Perimeter Defences & Physical Access Mechanisms | Occupied buildings and LBG supporting IT infrastructure are protected by proportionate perimeter defences (e.g. fences, cable distribution systems), deterrents (e.g. CCTV), and physical access mechanisms (e.g. locks, access control readers & cards, security guards, access control vestibules (mantraps)) to prevent unauthorised access, theft of information, tampering or sabotage of IT equipment. |

| | |
|---|---|
| Physical Intrusion Detection | Occupied buildings, and hosted events (e.g. AGM) have physical intrusion detection capabilities (e.g. CCTV, intruder alarm systems, security officers etc.) to detect unauthorised access and to prevent the theft of information, tampering or sabotage of IT equipment. |
| Training, Awareness & Capability | External Supplier colleagues receive tailored security education, awareness, and training relevant to their role, enhancing their understanding of security threats, roles, responsibilities, and acceptable usage of technology and information to help prevent against theft, leakage, manipulation, destruction, unauthorised or loss of access to information. |
| External Supplier Security Control Assurance | Products and services from External Suppliers and other third parties have minimum expectations for security integrated into the procurement process.<br>Adherence to contractual security obligations and the Security Policy is monitored, assessed, and managed throughout the lifecycle of the third-party service to prevent adversaries exploiting security weaknesses in the supply chain |
| Non-Compliance | All requirements defined within this Risk Policy are applicable from the date of publication. Where requirements cannot be implemented within four weeks of the publication date, a temporary exception must be requested supported by an appropriate and timebound action plan.<br>Failure to comply with the live, published version of this Risk Policy may result in remedial actions, formal escalation, and potential contractual consequences, including restriction, suspension, or termination of the supplier relationship. |

# 10. DATA & PRIVACY RISK POLICY REQUIREMENTS

The risk of inappropriate use or management of data in the course of delivering customer / colleague and business objectives.

| Requirement | Description |
|---|---|
| Purpose | These Data & Privacy Risk Policy requirements set out the expectations that external suppliers must meet when processing data for Lloyds Banking Group, regardless of the data's origin. Their purpose is to ensure that all external supplier activities for the Group involving data are managed, protected, and governed in line with Lloyds Banking Group's risk appetite, regulatory obligations, and contractual commitments. By complying with these requirements, external suppliers help to ensure effective management of data and privacy risks throughout the data lifecycle, safeguarding the rights and interests of both customers and the Group. |
| Applicability | These policy requirements apply to all external suppliers who process, store, access, or manage data on behalf of Lloyds Banking Group, irrespective of the nature of the service, the data format or origin of the data. External suppliers are required to comply with the applicable requirements set out in this policy and any additional contractual obligations agreed with Lloyds Banking Group.<br><br>External suppliers operating outside the UK must ensure that local country and jurisdictional legislation and regulatory requirements are adopted in addition to the requirements below.<br><br>Local laws or regulations will take precedence. As such, where these laws or rules conflict with, or result in, any requirements not being fulfilled, or where any of the requirements prohibit an activity that is mandatory under local law, the external supplier must inform the Group to agree what actions should be taken. |
| Scope | The policy requirements apply to all data processed by external suppliers on behalf of Lloyds Banking Group, regardless of origin. This applies to all data formats, including structured, unstructured, and physical data, and to the entire data lifecycle while external suppliers are processing or retaining data for LBG.<br><br>The policy requirements are technology-agnostic and applies across all tools and systems, including emerging and advanced technologies, such as Artificial Intelligence.<br><br>Where external suppliers are unable to meet a requirement, they must notify their Supplier Manager without delay. The Supplier Manager must engage the Policy Owner to agree an alternative compliant approach. |
| Metadata & Data Lineage | Accurate and comprehensive metadata and data lineage is documented and maintained. This increases confidence in data by providing transparency and understanding of data flows. Additionally, it ensures data accuracy, completeness, reliability, and compliance with regulatory requirements. |
| Data Quality | Clear data quality requirements and target thresholds for data are established and documented. This ensures that data quality standards are consistently applied and met for Lloyds Banking Group's data, supporting reliable and accurate data usage.<br><br>Mechanisms and controls are embedded into technologies and processes to understand and manage the structure, content, and quality of data. This supports the identification and prevention of data quality issues, enabling targeted improvements and maintaining data integrity throughout the lifecycle. Methods may vary depending on the supplier's systems and capabilities.<br><br>Lloyds Banking Group are informed of any identified issues with the quality of our data as soon as they are detected. This proactive communication supports |

| | |
|---|---|
| | the timely resolution of data inaccuracies, ensuring data accuracy, completeness, and reliability. |
| Data Privacy | Personal Data is processed lawfully, fairly and in a transparent manner. This helps individuals understand how their Personal Data is used and ensures we follow regulatory requirements.<br><br>Personal Data is collected for specified, clear and legitimate purposes. Where Personal Data is to be used again, but for a new purpose, we first assess the lawfulness, fairness, and transparency of any further processing. This is essential to maintain trust, ensures transparency and prevents misuse of individuals' data.<br><br>Processing of Personal Data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. This minimises the amount of Personal Data processed reducing the risk of misuse.<br><br>Personal Data is accurate and kept up to date. This means steps must be taken to ensure the maintenance of accurate Personal Data and rectification of any inaccurate data immediately.<br><br>Personal Data is kept for no longer than is necessary. This helps reduce the risk of misuse, unauthorised access or use outdated Personal Data.<br><br>Processes are in place that respect and facilitate the exercise of individual's rights allowing for a response or action to be taken within required timescales. This allows individuals to retain effective control over their Personal Data, supports fair and responsible processing and creates greater trust.<br><br>Records of Processing of Personal Data are documented and kept up to date. This provides a record of our Personal Data processing activities.<br><br>Processing that is likely to result in a high risk to the rights and freedoms of individuals is identified and subject to a Data Protection Impact Assessment (DPIA). When acting as a data controller, a DPIA is undertaken. When acting as a data processor, sufficient information and support is provided to Lloyds Banking Group to enable completion of their DPIA. This ensures that any potential risks and harms this processing could have to an individual are identified and mitigated, demonstrating a proactive approach to safeguarding their privacy and security.<br><br>All actual or suspected Personal Data breaches are reported via the Lloyds Banking Group Supplier Manager / Service Manager as soon as identified and no more than 24 hours after discovery, or in line with agreed contractual obligations. Assistance is provided, where required, to document the breach and support any notification to the relevant Supervisory Authority. This ensures priority is given to assessing and mitigating actual and potential harms to individuals and ensures that they are appropriately supported.<br><br>Electronic communications involving marketing and tracking technologies, including Cookies, are assessed to ensure they are lawful, fair and transparent. This supports responsible digital practices, helps our digital users understand what tracking technologies we use and why, and protects individual rights. |
| Storage Retention and Disposal | Data and Records are stored in reliable storage, suitable for their type, processing, retention, and access requirements. This supports compliance with regulatory requirements and ensures Data and Records are managed through their lifecycle.<br><br>Personal Data and Records are not stored, processed, or accessed in jurisdictions that Lloyds Banking Group has identified as posing material legal, regulatory, or operational risk. This requirement supports compliance with applicable laws, protects against data misuse or loss, and ensures operational resilience by maintaining control over data handling locations.<br><br>Inactive Data and Records—defined as those no longer required for routine business activities and not subject to frequent access or retrieval (e.g. daily/monthly)—are archived or stored in non-production environments on a |

| | |
|---|---|
| | regular basis. This prevents inactive data from being unnecessarily processed, and ensures active data remains easily accessible and manageable.<br><br>Retention periods for Data and Records are agreed up front with the Group as part of contractual agreements. This ensures compliance with legal and regulatory requirements, reduces storage costs, and mitigates risks associated with data breaches and outdated information.<br><br>Methods are implemented to enable the timely and compliant disposal of Data and Records once their retention period has ended. This ensures Data and Records are not retained longer than required, and reducing the risk of using or relying on outdated Data and Records.<br><br>Data and Records which are required for anticipated or ongoing regulatory action or legal disputes are identified and preserved. This ensures all Data and Records are kept safe and available for legal proceedings, helping the Group respond effectively and meet legal requirements. By specifying only the necessary scope, blanket holds are avoided, promoting efficient data management.<br><br>All data sharing arrangements are documented, with appropriate agreements and technical safeguards in place to protect any data transferred to external suppliers. Where data is transferred across jurisdictions, a lawful transfer mechanism is established, and the associated risks of processing data in another jurisdiction assessed.<br><br>In agreement with the Group, upon exit, return or disposal of Group Data and Records. This ensures compliance with contractual obligations, protects sensitive information, and supports efficient data management practices. |
| Unauthorised Data Usage | Lloyds Banking Group Data must not be used by external suppliers, or their supply chains, to train, fine tune, validate, or improve artificial intelligence, machine learning, large language models, or similar technologies unless explicitly agreed in advance as part of a contractual arrangement with Lloyds Banking Group. This prevents unauthorised secondary use of Group Data, supports purpose limitation and confidentiality obligations, and reduces the risk of loss of control, customer harm, or regulatory non-compliance. |
| Training | The external supplier must ensure all employees/contractors responsible for complying with these Data & Privacy policy requirements complete appropriate Data & Privacy training. This is to ensure external supplier employees/contractors understand how the policy requirements and relevant data legislation affect their role and their responsibilities. |

# 11. External Supplier Risk Policy Requirements

These requirements must be followed to manage the risks associated with the inappropriate and / or inadequate selection, onboarding, management or off boarding of services received by any part of the Group from external suppliers and their supply chains.

| Requirement | Description |
|---|---|
| Purpose | When an external supplier to Lloyds Banking Group ('the Group') sub-contracts part of the contracted services to its own supplier(s), we expect them to ensure that these subcontractors operate to the standards expected by the Group.<br>To achieve this, external suppliers should adhere to the minimum requirements outlined below, adopting a risk proportionate approach, i.e. the greatest level of control and oversight should be in place for those sub-contractor arrangements assessed as carrying the most risk. |
| Applicability | External suppliers operating outside the UK must ensure that local country and jurisdictional legislation and regulatory requirements are adopted in addition to the requirements below.<br>Local laws or regulations must take precedence. As such, where these laws or rules conflict with, or result in, any requirements not being fulfilled, or where any of the requirements prohibit an activity that is mandatory under local law, the external supplier must inform the Group to agree what actions should be taken. |
| Scope | Any third-party supplier contracted to provide goods and services to Lloyds Banking Group that sub-contracts any part of the contracted services to its own supplier(s) is in scope of the below External Supplier Requirements |
| Doing Business Responsibly | Comply with the Group's Code of Supplier Responsibility. |
| Sub-contracting | Notify the Group of any intention to sub-contract any part of a contracted arrangement to a supplier(s). Where the use of such sub-contractors is agreed by the Group, ensure the Group is kept up to date on the supplier information by submitting the Nth Party Questionnaire when requested. |
| Roles & Responsibilities | Define and agree roles and responsibilities so that the split of responsibility between you and your sub-contractors for the scope of the goods and services to the Group is clearly articulated and understood by the Group. |
| Risk Assessment | Classify sub-contractors based on the level of risk posed and manage them proportionately to this and any ongoing risk assessments. |
| Due Diligence | Perform appropriate and proportionate due diligence on your sub-contractors before onboarding them and on an ongoing basis. |
| Compliance with Group Policies | Where invited to do so by the Group, via its external partner Hellios, complete the Group's Financial Supplier Qualification System (FSQS) annually to confirm minimum Group policy requirements are met. |
| Concentration Risk | Assess, monitor and manage any concentration risks in your supply chain, including multiple arrangements with the same or closely connected suppliers; where multiple otherwise unconnected service providers depend on the same external supplier for the delivery of their services; arrangements with service providers that are difficult or impossible to substitute; and dependencies in a close geographical location. The external supplier must periodically inform the Group on the concentration risk position and where applicable agree what actions should be taken. |

| | |
|---|---|
| Supply Chain Performance | Have an appropriate, consistent and reportable approach to supplier management, ensuring it is followed to manage the written agreement obligations on both sides and the operational performance of suppliers. |
| Supplier Risk Management | Have an appropriate approach to sub-contractor risk management which ensures the Group's risk and control environment is not materially weakened and does not adversely affect the ability of the regulators to monitor the Group's compliance with its regulatory obligations. As a minimum this should include:<br>• The operation and assessment of sub-contractor controls in place to meet Group requirements.<br>• The management, monitoring and reporting of risks and issues to the Group.<br>• Undertaking a periodic assessment of sub-contractor controls, policies and standards. |
| Supplier Assurance | Undertake ongoing assurance of any sub-contractors which could impact the goods and/or services you provide to the Group. The external supplier must periodically inform the Group on the results of assurance work and where applicable the actions being taken. |
| Audits | Support any audit and assurance activity and resulting actions, including activities by regulatory and competent bodies, in line with the written agreement. Ensure sufficient resource is made available to support any reasonable request, if required. |
| Business Continuity & Exit Planning | Have a robust contingency in place to ensure the continuation of service to the Group. Where required by the Group, this should be as part of an agreed, documented and tested exit plan that aligns to any supplier business continuity planning. |
| General Termination | The termination of arrangements with your sub-contractors that come to the end of their tenure and do not require renewal is done in a controlled manner, in compliance with any termination clauses in the written agreement, ensuring continued compliance with other Group policies (e.g. data retention) and notifying the Group of the termination. |

# 12. FINANCIAL REPORTING & TAX POLICY REQUIREMENTS

The risk of a material misstatement or error within the Group's external financial and tax reporting, regulatory reporting (financial), or internal financial and tax management reporting.

| Requirement | Description |
|---|---|
| Purpose | This Policy sets out the financial reporting and tax risk requirements that suppliers providing services to Lloyds Banking Group (LBG) must support and comply with where relevant to the services they deliver. Its purpose is to help ensure the integrity of financial, regulatory and tax reporting, support compliance with applicable laws and regulations, and minimise the risk of reporting errors or tax non-compliance arising from supplier activities. |
| Applicability | Third parties must ensure:<br>• Financial reporting and tax services including the provision of data comply with contractual agreements.<br>• Financial reporting and tax services including the provision of data are compliant with local, international, statutory, legislative, contractual and regulatory requirements. |
| Scope | The Financial Reporting and Tax Risk Policy are applicable to third parties who are involved in end-to-end reporting processes across the Group. This is usually in the capacity of service providers i.e. 'service organisations', data providers or system providers as follows:<br>• Service providers: The external supplier performs functions which are an integral part of financial control or calculates financial data on behalf of LBG.<br>• Data providers: Industry wide data providers; or where LBG is reliant on the data for financial reporting processes.<br>• System providers: Provide external suppliers systems 'off the shelf' e.g. hosting data and standard business processes. |
| Service Organisation Controls Report (SOC) | Where an external supplier is considered to be a service provider, supporting financial reporting processes, assurance over the design and operating effectiveness of third-party controls will be performed by the external supplier's independent auditor and results shared with 'user entities' in a Service Organisation Controls (SOC) report. User entities are LBG legal entities who are impacted by the SOC reports. There are several types of SOC report - the two which are likely to be most relevant are:<br>• The SOC1 report involves the service organisation's independent auditor's assessment of the design and operating effectiveness of the Internal Controls over Financial Reporting (ICFR) at the service organisation. Typically, this will be a SOC1 Type 2 report which covers a period, usually 12 months and will test the design and operating effectiveness of controls over this period.<br>• The scope of the SOC1 Type 2 report will specify the ICFR which are relevant to the services which are being provided by the external supplier for example IT general controls, model governance, controlled change etc.<br>• A SOC 2 report may be provided which focuses on controls at the service organisation relating to security, availability, confidentially and processing integrity for the systems used by the service organisation. |
| Compliance with Applicable Laws, Regulations and Accounting Standards | Third parties will prepare in scope reporting in accordance with relevant standards (which incorporates compliance requirements with applicable law and appropriate regulations).<br>Examples of applicable laws and regulations (this list is not exhaustive): |

| | |
|---|---|
| | • UK Companies Act 2006<br>• International Financial Reporting Standards (IFRS)<br>• UK Corporate Governance Code<br>• PRA Rulebook<br>• UK Corporation Tax Acts and Finance Acts |
| Tax liabilities and reporting obligations | The calculation, payment and filing of any tax liabilities or reporting obligations to tax authorities must be complete, accurate and timely. |
| Technical judgements | Tax technical judgements made, must not result in reputational damage for LBG Group as a consequence of the tax position. |
| Documentation Procedures and Controls. | Third parties will ensure procedures and controls are in place for the preparation of financial reporting and tax data and /or calculations on behalf of LBG to support the completeness, accuracy and timeliness of data included in financial and tax reporting. |
| Assurance | External Supplier service providers will provide independent assurance reports to LBG e.g. SOC reports and a bridging letter where relevant to the required timescales to support financial reporting and tax activity and in line with contractual agreements.<br>Third parties will provide information to support independent audit (non-statutory) or assurance activity relevant to their data and /or calculations as required per contractual agreements. |

# 13. FRAUD RISK POLICY REQUIREMENTS

These requirements must be followed to manage the risk that the Group implements ineffective systems, processes and controls to prevent, detect, respond and remediate the risk of internal or external fraud.

| Requirement | Description |
|---|---|
| Purpose | This policy sets out clear rules for suppliers to help prevent, detect, and respond to fraud. It ensures everyone is accountable, that fraud risks are identified and managed, and that lessons are learned from any incidents. The requirements are based on UK law and other relevant regulations, but suppliers must follow stricter local laws if applicable. |
| Applicability | This policy is for third-party suppliers—companies or individuals who provide goods or services to the Group (the organization).<br>It applies when the Group has decided that its main fraud policy should also cover the supplier's work. |
| Scope | The policy covers three main types of fraud: customer fraud, external fraud, and internal fraud.<br>Types of Fraud Explained:<br>Customer Fraud<br>• This is when a customer is tricked into making a payment because they misunderstand the situation. For example, someone might convince a customer to send money by pretending to be someone else or by creating a false emergency.<br>• In the UK, this is often called Authorised Push Payment (APP) fraud—where the customer authorizes the payment but has been deceived.<br>External Fraud<br>• 1st Party Fraud: The customer themselves tries to commit fraud using their own accounts or products.<br>• 3rd Party Fraud: Someone who is not a customer uses a customer's details to try to commit fraud. For example, a criminal might steal a customer's identity and use it to access accounts.<br>Internal Fraud<br>• This is fraud committed by people inside the organization or those connected to it, such as:<br>• Employees (permanent, temporary, contract, or agency staff)<br>• Suppliers and their employees<br>• Business introducers (people who bring in new business)<br>Internal fraud includes:<br>• Using trust or access to assets for unauthorized or illegal purposes.<br>• Fraud intended to benefit colleagues, suppliers, introducers, third parties, or customers.<br>• Fraud intended to benefit the Group itself, either directly or indirectly.<br>• Helping others commit fraud by being reckless or intentionally ignoring suspicious activity—even if not directly involved. |

| | |
|---|---|
| Due Diligence | Perform appropriate and proportionate due diligence on your sub-contractors before onboarding them and on an ongoing basis. |
| External suppliers must ensure: | Fraud controls are operated across the PREVENT, DETECT, RESPOND AND REMEDIATE principles (see below for more details on the principles). These controls must be appropriate and relevant to the type of business and proportionate to the fraud risk;<br><br>Sample checking is undertaken to ensure employees adhere to key fraud processes across the PREVENT, DETECT, RESPOND AND REMEDIATE principles. Details of key fraud processes checked, and all findings must be shared with the Group's supplier manager on request;<br><br>Ongoing control testing/assurance plans are in place to monitor the effectiveness of fraud controls across the PREVENT, DETECT, RESPOND AND REMEDIATE principles. Details and results of fraud control effectiveness monitoring must be shared with the Group's supplier manager on request;<br><br>Effective compliance with this Policy, identifying where remediation is required and implementing agreed actions. This includes identification of fraud risks, changes in fraud risks, events, control failings and/or Policy breaches. Where these impact the Group or its customers, they must be reported promptly to the supplier manager or nominated Group contact and a full programme of remediation activity undertaken to resolve the breach. Details of findings in relation to compliance with this Policy must be shared with the Group's supplier manager proactively;<br><br>Detailed Root Cause Analysis (RCA) is undertaken upon the identification of a fraud event. The RCA should establish if any control principles were breached. Results and remediation plans must be shared with the Group's supplier manager proactively;<br><br>New employees/contractors must complete their fraud training within 8 weeks of employment, and prior to undertaking any task that may impact the Group or its customers, e.g. amending/initiating payments, managing Group data, or handling Group cash;<br><br>Fraud training must be completed by all employees/contractors on an annual basis, unless there are appropriate reasons for non-completion, e.g. Maternity Leave, or Long-Term Sickness.<br><br>Where employees/contractors are identified as working in roles considered high risk for fraud, role specific training should be considered to ensure that they are aware as to the increased fraud risks associated with their roles.<br><br>Regular MI on fraud training completion rates for all employees are recorded. This MI must be made available upon request by the Group's supplier manager. |
| Fraud Policy | External suppliers must document their approach to the following PREVENT, DETECT, RESPOND AND REMEDIATE principles in their own Fraud Policy. The approach must detail the systems, controls and processes that are operated to manage the risk of fraud.<br><br>The Fraud Policy must:<br><br>• Be proportionate to the fraud risk, as identified through a risk assessment exercise;<br><br>• Be appropriate and relevant for the type of business;<br><br>• Cover all types of fraud risk: i.e. external, and customer fraud. This also includes fraud intended to benefit the Group, directly or indirectly.<br><br>• Be reviewed regularly, at least annually, or upon changes to the systems, controls and/or processes to ensure they remain up to date.<br><br>• Be shared with the supplier manager on request. |

| | |
|---|---|
| | • Document the controls operated in respect of the principles of this Policy, detailed below. This must specifically include the expected triggers, levels of accountability and responsibilities for action.<br>• Include a fraud response plan; and<br>• Document the reporting and escalation processes that must be followed upon discovery of a suspected or actual fraud, including when you advise the Group. |
| Prevent Fraud | External Suppliers must ensure fraud threats are identified and fraud risks are mitigated through maintaining effective systems, controls and processes, prior to establishing a relationship and during the lifecycle of that relationship.<br>The third-party supplier must operate controls in respect of the following (but not limited to) where it is applicable to the third-party supplier:<br>• ID Validation (IDV): proving that someone, or a company, is who they say they are and reside where they say they do when we have no existing relationship with them. This must include compliance with the pre-employment vetting check requirements detailed in the People Policy – External Supplier Requirements;<br>• Assessing Entities & Relationships: ensuring that, once a person or company has been identified, the potential fraud risks are assessed before entering into a relationship with them and throughout the lifecycle of the relationship.<br>• Authentication: ensuring controls are in place to minimise the risk of unauthorised access. All interactions must be scored based on the potential risk of interaction. Interactions involving the payment of funds will require a higher level of authentication. Further information can be sourced via the supplier manager.<br>• Data & Intelligence Sharing: ensuring fraud risk data and intelligence is proactively shared between the Group and the third-party supplier.<br>• Preventing Internal Fraud: ensuring effective controls are in place to prevent internal fraud, supporting the Group's zero appetite for internal fraud; and<br>• Education and Awareness: ensuring the third-party supplier provides customers and employees with information, either face to face, online, via a web page or a variety of methods to help them in protecting themselves against fraud. This should must include keeping customers and employees abreast of current fraud threats or scams and providing guidance on when and how to report fraud. The third-party supplier should must also ensure its employees are made aware of the Group's zero appetite for internal fraud, including fraud intended to benefit the Group either directly or indirectly |
| Detect Fraud | External Suppliers must ensure fraud events are effectively identified and managed through maintaining effective systems, controls and processes, during the lifecycle of that relationship.<br>The third-party supplier must operate controls in respect of the following (but not limited to) where it is applicable to the supplier:<br>• Channel Protection: ensuring that channels used to deliver products and services are resilient to fraud, for example the provision of Malware defences on online service channels.<br>• Activity & Transaction Monitoring: ensuring suspicious transactional activity is monitored and alerted; and<br>• Detecting Internal Fraud: ensuring staff activity is monitored and all suspicious activity is alerted to the supplier manager. |
| Respond to Fraud | External Suppliers must ensure maintenance of a clear Fraud Policy enabling the supplier to react to fraud and suspected fraud events in a timely manner when they occur. |

| | |
|---|---|
| | The third-party supplier must operate controls in respect of the following (but not limited to) where it is applicable to the supplier:<br>• Customer Vulnerability: ensuring an appropriate response to customers identified as vulnerable.<br>• Duped and Scammed Customers: ensuring an appropriate response to customers identified as victims of fraud.<br>• Support to Customers and employees: ensuring customers and employees are aware of who they should contact in the event of fraud.<br>• Reporting Fraud Performance: ensuring management information is made available in a timely manner to the supplier manager relating to customers impacted by fraud and fraud prevention activity.<br>• Regulatory and Media Requests: ensuring any such incidents are referred to the supplier manager in a timely manner; and<br>• Recovery: ensuring clear articulation of roles, responsibilities, processes and procedures to support the recovery of funds. |
| Remediate Fraud | External Suppliers must ensure appropriate corrective actions are undertaken and root cause analysis completed where appropriate to reduce the future impacts of fraud on both the Group and its customers.<br>The third-party supplier must operate controls in respect of the following (but not limited to) where it is applicable to the supplier:<br>• Escalation and Reporting of Fraud Cases: ensuring clear lines of responsibility for both the third-party supplier and the Group in managing and reporting fraud cases to ensure swift reporting of non-compliance, loss and control failings that could impact Group or customer assets.<br>• Root Cause Analysis: ensuring processes are in place to undertake root cause analysis and to identify the point of compromise and point of exit; and<br>• Exit of Relationship: ensuring processes are in place to respond to staff fraud events, including clear criteria for seeking employee dismissal |
| Failure to Prevent Fraud | External Suppliers must implement robust systems and controls to prevent fraud. These requirements are aligned with UK Home Office guidelines and the Financial Conduct Authority (FCA) expectations for effective control frameworks.<br>Suppliers must ensure their fraud prevention measures cover the following six principles:<br>Top Level Commitment:<br>• Senior management must actively support and lead anti-fraud efforts, setting a clear tone that fraud will not be tolerated.<br>Risk Assessment:<br>• Suppliers must regularly assess where fraud risks exist in their operations and identify areas most vulnerable to fraud.<br>Proportionate Risk-Based Fraud Prevention Procedures:<br>• Controls and procedures must be appropriate to the level of risk—stronger controls for higher-risk areas, and proportionate measures elsewhere.<br>Due Diligence:<br>• Suppliers must verify the integrity and trustworthiness of their own staff and any subcontractors or associated persons.<br>Communication:<br>• Anti-fraud policies and expectations must be clearly communicated to all relevant staff and third parties, including training where necessary. |

| | |
|---|---|
| | Monitoring & Review:<br>• Suppliers must regularly monitor and review their fraud prevention measures to ensure they remain effective and up to date. |
| Management MI | External Suppliers must ensure that key fraud management information is produced, and evidence is available by the Group Supplier Manager. |
| Non-Compliance | Any material differences between the requirements set out above and the supplier's own controls must be raised by the supplier with the Group's Supplier Manager.<br>The supplier manager will then discuss the non-compliance with the accountable executive for the relationship and local Risk team to agree a way forward. |

# 14. GIFTS, ENTERTAINMENT & HOSPITALITY POLICY REQUIREMENTS

These requirements must be followed to manage Gifts, Entertainment & Hospitality Risk and adhere to regulatory requirements and expectations.

| Requirement | Description |
|---|---|
| Purpose | Gifts, Entertainment & Hospitality refers to the provision of gifts, or hospitality/entertainment where no fee is paid in return by the recipient. These activities are often used to build relationships but can be a risk for bribery or corruption and create conflicts of interest. |
| Applicability | The Gifts, Entertainment & Hospitality policy applies to third parties of Lloyds Banking Group ('the Group'), to the extent that they are involved in regulated activities relating to the Group's customers. If the external supplier is not involved in regulated activities relating to the Group's customers, it is considered out of scope of the policy. |
| Scope | Gifts, Entertainment & Hospitality (GEH) arrangements should cover:<br>• Offering or giving of GEH to third parties<br>• Receiving or accepting GEH from third parties. |
| Recording and effective management of Gifts, Entertainment & Hospitality | Such third parties must maintain a register of Gifts, Entertainment and Hospitality (GEH) and be able to demonstrate that any GEH given or received could not be seen to be as a bribe or create a conflict of interest. Staff should be aware of their requirements relating to GEH. The register should contain sufficient information to be able to understand the nature, value, recipient and authorisation. The register must be reviewed periodically by an appropriately senior owner at the supplier and be available to the Group upon request. GEH, other than inconsequential items such as refreshments, is unlikely to be deemed appropriate whilst there are contract negotiations or tenders underway or imminent. |

# 15. HEALTH, SAFETY, PERSONAL SECURITY & PREMISES RISKS POLICY REQUIREMENTS

Supplier Onboarding: Health and Safety Principles

| Requirement | Description |
|---|---|
| Purpose | The purpose of this section is to define the minimum Health, Safety, Personal Security and Premises requirements that external suppliers must meet when delivering services for, or on behalf of, Lloyds Banking Group. These requirements are designed to ensure the safety of colleagues, customers and third parties, and to protect the Group's premises and operations. |
| Applicability | This section applies to all external suppliers, contractors and service providers engaged by Lloyds Banking Group, including those whose activities:<br>• Are undertaken on Lloyds Banking Group sites or premises<br>• May impact Lloyds Banking Group colleagues, customers or property<br>• Involve the provision of services, goods or works where Health and Safety risks may arise<br>All requirements set out within this section are mandatory for any supplier, contractor or service provider working on behalf of Lloyds Banking Group and must be met prior to engagement and continuously throughout service delivery. |
| Scope | External suppliers play a critical role in supporting Lloyds Banking Group (LBG). To protect our people, customers, and workplaces, all suppliers must operate safely, responsibly, and in compliance with our Group Health, safety, environmental and premises principles, including the LBG Health & Safety Policy, a copy of which can be obtained from the relevant Supplier Manager. |
| Core Supplier Responsibilities | Maintain an up-to-date Health and Safety Policy and management system covering all activities and services.<br>Comply with all applicable local Health, Safety, Environmental, Fire, Premises, and construction legislation.<br>Provide goods, equipment, and materials that are safe, fit for purpose, and legally compliant.<br>Ensure workers are trained, competent, and authorised for their assigned tasks.<br>Define clear Health and Safety roles and responsibilities aligned to organisational structure and supplier duties.<br>Suppliers must ensure that all individuals undertaking activities are appropriately trained and competent prior to commencing work, with training relevant to their role, the activities being undertaken and the associated risks. This must include, where applicable, induction, role-specific, site-specific and refresher training. Training must be completed prior to undertaking activities and maintained at defined and appropriate intervals, determined in line with applicable legal, regulatory and recognised industry standards. Evidence of training completion, competence and authorisation must be retained and made available upon request.<br>Allocate adequate resources proportionate to the size, nature, and risk of the activities undertaken. |
| Risk Management Requirements | Comply with Lloyds Banking Group Health and Safety requirements prior to commencing work and when working on, or representing, LBG locations.<br>Provide suitable and approved risk assessments identifying hazards, impacts, affected persons, and control measures. |

| | |
|---|---|
| | Maintain safe working environments through effective control measures.<br><br>Ensure that risk assessments and associated control measures are reviewed, approved and implemented prior to commencing work, and are aligned to applicable legislation and recognised industry standards.<br><br>Maintain control frameworks, processes and working practices that meet or exceed relevant legal requirements and recognised industry standards, and demonstrate this through appropriate assurance, certification or independent verification where required. |
| Working Safely on LBG Sites | Safe Systems of Work and Permits to Work must be established and applied in accordance with Lloyds Banking Group standards, site procedures or other formally agreed control frameworks appropriate to the activity being undertaken.<br><br>Use appropriate Permits to Work for high-risk tasks, including hot works, electrical works, confined spaces, working at height, excavations, isolations, and associated activities. As per risk assessment and safe system of work.<br><br>Follow asbestos management arrangements and stop work immediately if suspect materials are identified.<br><br>Complete all site inductions, follow emergency procedures, and comply with site security protocols (sign-in/out, access control).<br><br>Prevent pollution and manage environmental impacts responsibly and in line with environmental compliance requirements. |
| Reporting & Assurance | Report incidents, near misses, and serious events in line with Lloyds Banking Group reporting requirements.<br><br>Disclose enforcement notices or regulatory actions promptly, whether received or pending.<br><br>Cooperate with audits, inspections, and assurance activities as required.<br><br>Stop work immediately where unsafe conditions are identified.<br><br>Health and Safety policies are communicated via established channels, including intranet, email, and supplier onboarding/inductions.<br><br>Safe Contractor and other procurement Safety Scheme requirements apply where relevant, with appropriate accreditation or equivalent assurance maintained throughout service delivery.<br><br>Fourth-party Health and Safety compliance is managed through contractual flow-down and ongoing monitoring.<br><br>Where suppliers use automated systems or emerging technologies (including artificial intelligence), whether directly or through third parties or their supply chain, suppliers must ensure any associated Health, Safety, Fire, Premises or Environmental risks are identified, assessed and effectively managed in line with Lloyds Banking Group requirements.<br><br>Suppliers must ensure that equivalent Health and Safety standards are applied across their subcontractors and wider supply chain, including through contractual obligations, monitoring and assurance activities proportionate to the risk.<br><br>Where a supplier identifies that it cannot fully comply with these requirements, the supplier must promptly notify the Lloyds Banking Group Supplier Manager, clearly outline the nature of the non-compliance, and agree an appropriate remediation plan and timeframe.<br><br>Any material non-compliance must be escalated in line with Lloyds Banking Group governance arrangements. |

# 16. IT SYSTEMS RISK POLICY REQUIREMENTS

The risk of disruption to our customer or business -critical IT service from IT failures, planned changes or human errors, data corruption, environment events, or third-party failures.

| Requirement | Description |
|---|---|
| Purpose | This Risk Policy sets out the consistent requirements and parameters which must be followed to manage IT Systems Risk within Lloyds Banking Group's approved Risk Appetite and enable compliance with all applicable regulation, legislation and associated standards that the Group must adhere to. Every External Supplier must know the Risk Policies that are relevant to their service and understand how to comply with these.<br><br>Technology is crucial to Lloyds Banking Group's (LBG) strategy, driving positive outcomes for our customers. Adhering to this Risk Policy boosts customer and stakeholder trust and strengthens operational resilience.<br><br>The key benefits are:<br><br>• Robust technology and top-tier data security build customer confidence and loyalty.<br><br>• Compliance with regulations and standards mitigates operational risks, ensuring stability and growth.<br><br>• Adhering to the Risk Policy reduces IT services disruptions and impacts from cyber threats, ensuring business continuity.<br><br>• A strong compliance foundation allows LBG to innovate freely, driving future growth and success.<br><br>This Risk Policy defines the key requirements that all External Suppliers and third parties must use to inform how they build and operate technology and manage IT System risk. Where required, the Risk Policy will be supported by guidance providing further detail on how to implement requirements and controls.<br><br>Technology is built to be resilient to a range of scenarios and without single points of failure where possible. Where this is not possible the associated risks are assessed and managed with appropriate mitigations, which are then documented within design documentation.<br><br>Implementation of the Risk Policy will also mean assessing whether preventative, detective and recovery controls mitigate the risk of IT service disruption within risk appetite (i.e. the degradation or full outage of a customer or business-critical IT service) whilst ensuring compliance with our legal, regulatory, and contractual obligations. |
| Applicability | All External Suppliers where they host, manage or provide technology which is used by the Group or its customers must adhere to the IT Systems Risk Policy |
| Scope | The scope of the IT Systems Risk Policy includes all technology-related activities, assets, and personnel within the External Supplier, including:<br><br>• Software and applications/workloads we write (including End User Developed Applications (EUDAs)), acquire (e.g. third-party software as a service), and maintain e.g. code, application programming interfaces (APIs), databases, and batch processing.<br><br>• Hardware and virtual/physical infrastructure we build, configure, and maintain to host applications e.g. compute, storage and networking, and branch devices. This includes on premise hosting environments and cloud landing zones (production and non-production).<br><br>• Utilities and tools we use to manage our applications / workloads and infrastructure services e.g. code repositories and development pipelines, |

| | |
|---|---|
| | asset and configuration management tools, and performance management tools.<br>• Technology vendors and third-party services the External Supplier consumes (including those mentioned above e.g. Software as a Service) |
| IT Asset Management | All IT assets are accurately inventoried, have ownership assigned, and are managed and maintained throughout their lifecycle for optimal utilisation, support recovery in the event of a disruption, and remain aligned with expectations to ensure compliance with legal, regulatory, and External Supplier obligations. |
| IT Change Management | All IT changes are categorised, impact assessed, developed (including backout plans), tested, implemented, and approved to reduce the risk of IT service issues. |
| IT Reliability and Redundancy (resilient by design) | To deliver appropriate levels of IT resilience, impact assessments and failure model analysis inform the reliability and redundancy requirements for IT systems. These requirements are explicitly accounted for in designs, validated through the quality assurance testing, and periodically proven in production. |
| IT Reliable Engineering | Engineering practices for IT systems (including software and infrastructure) apply automation, standardisation, and quality controls to support consistent, secure, and reliable builds. These practices prevent defects and promote service stability across environments. |
| IT Capacity Management | Capacity and performance requirements of IT systems are forecasted and monitored, and used to scale and meet future demand, to reduce the likelihood of reduced performance. |
| IT Performance Monitoring | IT systems are continuously monitored against service level agreements, with real-time alerts triggered upon detection of reduced performance or anomalies. |
| IT Incident & Problem Management | IT incidents & problems are identified, investigated, resolved, and reviewed for root cause to ensure timely restoration of IT services, reduce repeat occurrences and achieve service level agreements (recovery objectives for time and data loss & uptime). The External Supplier must periodically inform the Group of incidents and where applicable the actions being taken. |
| IT Backup & Restore Proving | Backup and restoration plans are proven to restore IT service within defined recovery objectives for time and data loss, following data corruption events. |
| IT Disaster Recovery Proving | IT Disaster Recovery plans are proven to restore IT service within defined recovery objectives for time and data loss following IT service disruptions. |
| External Supplier IT Control Assurance | Minimum expectations for technology are integrated into the procurement of products and services from external suppliers, monitoring External Supplier compliance to contractual obligations. |
| IT Training | External Supplier colleagues receive tailored technology education, training and awareness relevant to their role to ensure proficiency in the use of current and developing technologies to promote safe practices, enhance operational efficiency, and maintain regulatory compliance. |
| Non-Compliance | All requirements defined within this Risk Policy are applicable from the date of publication. Where requirements cannot be implemented within four weeks of the publication date, a temporary exception must be requested supported by an appropriate and timebound action plan.<br>Failure to comply with the live, published version of this Risk Policy may result in remedial actions, formal escalation, and potential contractual consequences, including restriction, suspension, or termination of the supplier relationship. |

# 17. MARKET CONDUCT POLICY REQUIREMENTS

Market Conduct Risk is defined as the risk that improper actions of firms or individuals' impacts market integrity through ineffective competition, improper market practices or insider trading.

| Requirement | Description |
|---|---|
| Purpose | This Risk Policy sets out the consistent requirements and parameters which must be followed to manage Market Conduct Risk and enable compliance with all applicable regulations, legislation and associated standards.<br><br>The term Market Conduct Risk is defined as the "the risk that improper actions of firms or individuals' impacts market integrity through ineffective competition, improper market practices or insider trading". Market Conduct Risk encompasses a broad range of risks such as (but not limited to) market abuse (e.g. insider trading and market manipulation), misleading disclosures, collusion, and other practices that distort the proper functioning, fairness and transparency of markets. |
| Applicability | Third parties which operate outside the UK must ensure that local country and jurisdictional legislation and regulatory requirements are adopted in addition to any Market Conduct Risk policy requirements.<br><br>Local laws or regulations must take precedence. As such, where these laws or rules conflict with, or result in, any requirements not being fulfilled, or where any of the policy requirements prohibit an activity that is mandatory under local law, the third party must inform the Group to agree what actions should be taken. |
| Scope | The Market Conduct Risk policy applies to third parties of Lloyds Banking Group ('the Group'), to the extent that they execute transactions in financial instruments on financial markets or are provided with inside information relating to Lloyds Banking Group, its customers, clients, transactions or market activities. |
| Policy Requirements | Such third parties must not engage in market abuse, improper market practices, unauthorised or inappropriate trading, or anti-competitive practices, must implement organisational arrangements, systems and procedures to prevent and detect market abuse and handle inside information in line with regulatory requirements. |

# 18. MODEL RISK POLICY REQUIREMENTS

The risk of adverse consequences from model errors and / or the inappropriate use of modelled outputs to inform business decisions.

| Requirement | Description |
|---|---|
| Purpose | To enable the appropriate management of model risk, the Policy requires suppliers to manage quantitative methods (QMs) in line with Group standards.<br><br>To achieve this, suppliers must adhere to the minimum standards outlined below. |
| Applicability | These requirements apply where a supplier provides a service to the Group and, in doing so, uses a QM, directly or indirectly, to generate, transform, or materially influence quantitative or qualitative outputs used by the Group. Suppliers are required to comply with the applicable requirements set out in this policy and any additional contractual obligations agreed with the Group.<br><br>This includes QMs that are:<br><br>• Used in delivering a service to the Group, including within the supplier's internal processes and systems; and<br><br>• Used directly or indirectly to support, inform, shape, or contribute to services, deliverables, advice, or analysis, whether or not outputs are provided to the Group.<br><br>This includes vendor built, vendor or internally hosted, customised, configured, off-the-shelf QMs, artificial intelligence (AI), Generative AI (GenAI), or Agentic AI components.<br><br>For the purposes of model risk requirements, 'supplier' includes any sub-contractors that suppliers use.<br><br>Where a supplier is unable to meet a requirement or cannot share the requested information, they must inform their Supplier Manager. The Supplier Manager should contact the Policy Owner where needed to agree an alternative compliant approach. |
| Scope | Defines the activities, processes, and risk areas associated with third-party provision and the use of QMs that influence Group decisions. This covers the full QM lifecycle and relevant supplier obligations. Excludes simple, transparent calculations that do not materially impact outcomes. |
| Definitions | Quantitative Method (QM) \| A QM is a quantitative calculation method, system, approach, end-user developed application (EUDA), and / or calculator.<br><br>Model \| A model is a quantitative method that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into output. All AI, GenAI, and Agentic AI systems, including those underpinned by Large Language Models (LLMs), fall within this definition.<br><br>In scope Deterministic Quantitative Method (DQM) \| A DQM is a quantitative method that is not classed as a model. It is included in the scope of these requirements where it, or its outputs, are used by the supplier to provide information or services that drive or support Group business decisions.<br><br>Group QM Stakeholders \| Group colleagues performing model risk management roles, including QM Owners, Developers, Implementation Engineers, Users, and Independent Validation and AI Risk Oversight Teams.<br><br>Artificial Intelligence (AI) \| AI refers to any system, model service, or component that performs tasks normally requiring human intelligence. This includes, but is not limited to:<br><br>• Machine learning, neural networks, deep learning. |

| | |
|---|---|
| | • GenAI, Agentic AI, and autonomous or semi-autonomous agents.<br>• Any solution underpinned by LLMs or similar foundation models.<br>This definition applies regardless of whether:<br>• The AI is developed by the supplier, licensed, embedded within another product, or accessed via an Application Programming Interface (API).<br>• The AI is used directly, indirectly, or as part of an automated or agentic workflow.<br>• The AI is static, configurable, fine-tuned, continually learning, or retrained over time.<br>• The AI is provided by the supplier or by a fourth party.<br>All such AI systems are considered QMs and are subject to all applicable model risk management requirements. |
| Roles & Responsibilities | The supplier must co-operate with Group QM Stakeholders by providing information, access, explanations and evidence required to fulfil the Group's responsibilities.<br>The supplier must have appropriately skilled personnel available to support oversight and challenge from the Group. |
| Documentation | To enable appropriate oversight of model risk, the supplier must provide sufficient documentation / information to allow the Group to understand the purpose, high-level design, operation, and limitations of any in-scope QMs or AI, Agentic AI and / or GenAI components they supply or influence.<br>Where full transparency is not feasible, alternative risk-based assurance may be provided, reflecting the materiality, complexity, and intended use of the QM, at the discretion of Group QM Stakeholders. |
| QM Identification | Where a supplier provides a service to the Group, the supplier must identify all QMs they provide or influence (e.g. through design, maintenance, or provision of outputs) and notify their Supplier Manager of their existence prior to use.<br>The supplier must provide sufficient information to support the Group's classification, ownership assignment, and inventory records. |
| Model Planning | The supplier must provide timely information, documentation, resource commitments, and technical detail required to support the Group's model planning process for any model delivered to the Group or any model outputs supplied to and relied upon by the Group. |
| Model Development | The supplier must supply sufficient documentation for the Group to understand methodology, assumptions, limitations, data, and performance.<br>Where full transparency cannot be provided, the supplier must explain constraints, assumptions and limitations, and provide alternative assurance appropriate to the risk. |
| Model Risk Classification | The supplier must provide sufficient information for the Group to assess model materiality, complexity, and other risk components, including limitations that may affect the level of risk that the QM poses.<br>Where supplier models or outputs are used across multiple Group entities, the supplier must support testing or provide evidence required for entity specific materiality assessments. |
| Model Approval | The supplier must provide artefacts, evidence, documentation, test results, and Subject Matter Expert (SME) access required to support the Group's model approval processes, including when a QM change is proposed.<br>The supplier must disclose usage conditions, constraints, limitations, or design boundaries that could restrict or influence the way the model may be used. |

| | |
|---|---|
| Model Implementation | The supplier must provide implementation artefacts and evidence to support safe deployment and testing by the Group. |
| Model Decommissioning | The supplier must assist the Group in the safe decommissioning of any model purchased from the supplier.<br>Where the supplier is decommissioning a model, the supplier must provide the Group with adequate assurance that decommissioning will not negatively impact upon the third-party service provided to the Group. |
| Model Monitoring and Maintenance | The supplier must provide monitoring outputs, issue notifications, or attestations as required where the Group cannot independently monitor performance.<br>The supplier must communicate emerging risks, degradation, or limitations in a timely manner. |
| Model Risk Mitigants | Where limitations or weaknesses require application of post-model adjustments (PMAs), restrictions on model use, or expert judgement overlays, the supplier must provide sufficient information for the Group to justify the temporary use of the mitigant, support its ongoing monitoring, and assess a clearly defined remediation plan. |
| Model Change | The supplier must notify the Group Model Owner of all model changes sufficiently in advance to allow review and, where required, challenge prior to implementation. This must include the rationale, testing evidence, and impact analysis.<br>The supplier must provide updated documentation reflecting the change, including assumptions, performance impacts, and configuration changes. |
| Independent Validation | The supplier must provide sufficient information, documentation, SME access, and evidence of their own independent validation activities to support the Group's independent validation processes.<br>Where code or full artefacts cannot be shared, the supplier must provide alternative evidence, including outputs, testing results, validation summaries, or supplier assurance reports. |
| AI Models (including GenAI and Agentic AI) | The supplier must provide information on training data, guardrails, controls, and limitations for any AI, GenAI, or Agentic AI component, recognising that these are models and subject to all applicable model risk requirements.<br>The supplier must identify, manage, and document risks arising from the use of AI models (including GenAI and Agentic AI) across the service lifecycle, including risks relating to output quality, reasoning, autonomy, and ongoing performance, such as hallucination, misinformation, misalignment, toxicity, and degradation over time.<br>The supplier must assess and mitigate bias arising from data, design, configuration, prompting, and use, including potential adverse impacts on different user groups. Where appropriate the supplier must maintain human oversight of AI outputs, with clear accountability, effective intervention or override mechanisms, and controls to avoid over-reliance on AI.<br>For AI systems with autonomous or agentic behaviour, the supplier must define boundaries of autonomy, govern how actions are initiated and executed, maintain enhanced monitoring (including drift and downstream impacts), and retain the ability to promptly restrict or disable the system where required.<br>The supplier must monitor for drift, including changes in data patterns, model behaviour, performance, or the effectiveness of controls, which may cause the AI system to become less accurate, reliable, secure, or aligned with its original purpose. |

| | |
|---|---|
| Deterministic Quantitative Methods (DQMs) | The supplier must provide sufficient documentation to understand the deterministic logic, inputs, outputs, assumptions and limitations of the DQM, and to support its identification as a DQM, inventory recording, and ongoing oversight. Not all stages of the model risk management process will be applicable to DQMs.<br><br>DQMs are out-of-scope of these requirements where they are simple calculations with transparency and limited logic used to support decisions (even if the decision is important). |

# 19. PAYMENTS & TRANSACTION EXECUTION (PTE) RISK POLICY REQUIREMENTS

The risk to the Lloyds Banking Group ('the Group') that mis-performance of payments or transaction execution (by colleagues, systems, robots or third parties operating on our behalf) have an impact on customers, clients, or internal operations.

| Requirement | Description |
|---|---|
| Purpose | The purpose of the PTE Policy is to enable external suppliers to effectively manage operational risks associated with the execution of transactions and the provision of payment services on behalf of the Group. This includes, but is not limited to, risks arising from failures to comply with Group policies, payment services regulations, Financial Market Infrastructure scheme rules, and applicable laws, codes of practice, and guidance from the European Banking Authority and local regulators. Beyond regulatory compliance, this Policy recognises that operational risks can also stem from process failures, system outages, human error, inadequate controls, or external threats. Such risks may result in service disruption, financial loss, poor customer outcomes, regulatory censure, and reputational damage to the Group. |
| Applicability | The PTE Policy applies to all external suppliers who execute transactions or provide 'Payment Services', infrastructure, or important operational functions supporting the Group's payment and transaction systems. External suppliers must also ensure compliance with all relevant jurisdictional legislation and regulatory requirements for the LBG entity they support and must also address broader operational risks as outlined in this Policy.<br>• For example, an external supplier supporting the provision of payment services for Lloyds Bank UK and Lloyds Bank in the Crown Dependencies (Jersey, Guernsey, Isle of Man) would need to comply with laws & regulations in the UK and each of the Crown Dependencies.<br>• Where jurisdictional laws or rules conflict with each other, or result in, any requirements not being fulfilled, or where any of the requirements prohibit an activity that is mandatory under the local law where the external supplier is based, the external supplier must inform the Group service owner who will liaise with the relevant Risk team(s) to agree what actions should be taken.<br>Applicability of individual requirements will depend on the service the external supplier is providing, and external suppliers should refer any questions to their service owner or usual business contact. |
| Scope | External suppliers should be aware of the following scope definitions:<br>• Transactions are the transfer of money or assets (e.g. the transfer of title deeds representing a real asset such as a house, or trading of stocks and shares). These transactions can be between a customer's own accounts, or with other parties to settle debts, fulfil financial commitments, or exchange for goods and services.<br>• Transactions do not include processes where there is no movement of money or assets, such as designing a new product or updating customer details.<br>Payments are a key type of transaction when a payer (sender) or payee (recipient) initiates the placement, transfer or withdrawal of money. Where this policy refers to transactions, this includes payments when sent or received. |

| | |
|---|---|
| | Some policy requirements only apply where the external supplier is providing 'Payment Services', infrastructure or important operational functions to support these for LBG entities operating in the United Kingdom (UK) or European Economic Area (EEA). Where this is the case, the external supplier must ensure compliance with payment scheme rules, payment legislation and / or regulations for the jurisdictions of the LBG entities they are providing services for. External suppliers which are not providing 'Payment Services' do not need to comply with these requirements.<br><br>External suppliers using AI Agents to execute customer transactions must ensure that these operate in line with this policy and provide outcomes that are at least the same as those delivered by trained staff, with appropriate controls, oversight, and monitoring of the Agent and transactions to prevent errors and/or customer harm. |
| Regulatory Permissions/Authorisations (UK & EEA Payment Services only) | External suppliers providing 'payment services' in their own right must have the regulatory permissions to perform the activity.<br><br>If external suppliers are acting as an agent of an Authorised Payment Institution (e.g. MBNA) they must not provide payment services until we have registered them on the FCA Register as our agent. |
| Digital Assets | External suppliers providing or supporting important operational functions for Digital Assets products may need to meet additional requirements which will be communicated by the Group. |
| Financial Market Infrastructure (FMI) and Payment Schemes | External suppliers executing transaction or supporting them (any operational functions for transactions) must meet any rules or codes set by FMI or Payment Schemes as the Group communicates to them (e.g. faster payments in the UK, Target in the EU). |
| Colleague Training and Capability Assessments | Individuals involved in transaction processing must complete sufficient training to be deemed competent for their role, including knowledge of any relevant payment regulations, legal or scheme requirements impacting the process they operate.<br><br>Ongoing competence must be assessed, monitored, maintained and records retained for evidence. |
| Access to Transaction Processing Systems | Adequate controls must be in place to manage access to systems used to execute transactions with appropriate segregation of duties enforced. |
| Payment Services Operational & Security Incident Reporting (UK Payment Services only) | External suppliers supporting UK entities must notify the Group via the service owner immediately of any 'payment services' incidents and support the Group in meeting the FCA requirement of reporting major incidents within 4 hours. |
| Management of Operational and Security Risks for Payment Services (UK & EEA Payment Services only) | External suppliers supporting UK entities must provide any information requested by the Group to support the FCA's requirement for assessing and reporting of Operational and Security Risks for Payment Services and the adequacy of mitigating controls. |
| Keeping Appropriate Records of Information Provided | External suppliers must keep records of individual transactions to evidence that the information required has been provided in line with any applicable regulation/legislation. |
| Standard Operating Procedures (SOPs) /Documented Processes | External suppliers must have documented standard operating procedures to provide employees with relevant step-by-step reference material supporting their transaction execution activity. This should include procedures to report incidents in a timely manner to the Group. |

| | |
|---|---|
| | Standard operating procedures must be regularly reviewed or if changes are required, such as changes to process, any associated regulations or scheme requirements.<br><br>SOPs must be approved by a suitable manager or delegate, kept version-controlled, and made easily accessible to all relevant staff<br><br>Any changes must be formally communicated to relevant staff. |
| Quality Checking | Where external suppliers are executing transactions they must define and implement risk-based quality checking to ensure SOPs, including any approval steps, are followed and effective.<br><br>The external supplier monitors quality checking records, addressing individual or thematic issues. Errors found must be corrected promptly with corrections reviewed independently to avoid repetition. |
| Authentication & Authorisation Checks | External suppliers must ensure that customers are authenticated before transactions are executed in line with the Group's authentication procedures.<br><br>Where an external supplier is providing authentication to access online banking services, make remote payments (e.g. card payments) or to enable other high-risk changes online (e.g. change of address) it must be able to demonstrate it meets Strong Customer Authentication standards. Where the external supplier adheres to a certification scheme it must confirm this is approved by the Group (such as FIDO) and the external supplier must be able to demonstrate it achieves the certification standard on a regular basis and when major changes are made.<br><br>External suppliers providing Open Banking services (e.g. Payment Initiation Service Provider (PISP) or Account Information Service Provider (AISP)) must apply Strong Customer Authentication (SCA) unless using an exemption. Any exemptions must be agreed with the Group before use via the Group service owner who will liaise with the relevant risk team(s). |
| Data Validation and Quality | Any systems or electronic forms used to capture transaction data must have validation rules for data accuracy. |
| Execution of Risk-Based Approval Processes | Risk-based approval checks are properly enforced before a transaction is executed and evidence retained. |
| Disclosing Fees, Charges and Currency Conversion | Where executing transactions, these are made in the currency agreed with the customer and the customer is informed of the maximum execution time and a breakdown of any charges, including any conversion charges and details of the exchange rate to be used (where available).<br><br>The customer is informed of any charges or cost reduction for using a particular payment instrument, either applied by the Group or another party, before the payment is made. |
| Open Banking (UK & EEA Payment Services only) | External suppliers providing AISP or PISP open banking services/supporting technology must provide availability and performance statistics on their interface to the Group via the service owner to support regulatory reporting. |
| Payment Services Complaints (UK & EEA Payment Services only) | External suppliers must support the Group to manage and respond to any 'payment services' complaints within 15 working days from receiving the complaint.<br><br>Complaints data must be shared with the Group as and when requested. |

| | |
|---|---|
| Having the Right Capacity to Execute Expected Volumes | External suppliers must ensure that they have the necessary capacity and capability to process transactions on behalf of the Group, planning for any anticipated spikes e.g. bank holidays and tax year end. |
| Sending and Crediting Transactions on Time | External suppliers must ensure that transactions are completed in line with any regulatory timescales and/or SLAs agreed with the Group via the service owner. Monitoring and MI must be available to demonstrate compliance with these timescales. |
| Execution of Transactions | The inability to execute any transaction must be notified to the Group via the service owner. |
| Card Transactions where the Amount is Unknown in Advance (UK & EEA Payment Services only) | For card transactions where the amount is not known in advance, an amount can be earmarked with the customer's authorisation.<br>Only the exact amount authorised by the customer can be earmarked.<br>Any earmarked amount above the final transaction value must be released immediately when the payment is made. |
| Transaction Identifiers and References | All transactions are assigned a unique identifier to enable identification later. |
| Avoiding Duplicate Transactions | Controls must be in place to identify and prevent transactions being duplicated. |
| Completeness Monitoring | End-to-end transaction journeys are monitored to ensure that, as a minimum, the volume and value (where applicable) requested through input channels is successfully processed to completion through downstream processes or systems. This should be real-time wherever possible, otherwise, at an intra-day frequency appropriate to the volume and value of transactions, potential impact of delayed execution and any time considerations (e.g. payments SLAs or scheme cut-offs).<br>Defined exception parameters trigger investigations into discrepancies to remediate any issues identified. |
| Risk Policy Breaches | Ensure the Group is immediately informed of any non-compliances along with any remedial actions taken to resolve the issue. Non compliances should be raised via the service owner who will liaise with the relevant Risk team(s). |
| Change Management | For changes impacting transaction or payment processing, a mapping exercise must be completed by the Change Programme to identify impact on any relevant payment regulation, law, scheme requirement, and/or industry standard.<br>Following the identification of any impact on payment regulation, law, scheme requirement, and/or industry standard, appropriate control must be implemented during the design and build phase to mitigate the risk of non-compliance. |
| Transaction Data Accuracy | Transaction data must be maintained throughout the transaction cycle from initiation to settlement. It should be processed as originally requested, in line with the applicable regulations, laws and scheme rules, and protected against undetected changes.<br>Where there is a need to fix an error or following a validated customer request to amend the transaction, a clear audit trail must be kept evidencing this. |
| MI and Reporting | Transaction execution performance monitoring MI must be in place and reported to the Group against agreed SLAs to evidence compliance with this Policy. Where outside of these agreed SLAs, |

| | |
|---|---|
| | effective action plans must be in place to resolve this, and progress reported to the Group via the service owner. |

# 20. People Risk Policy – External Supplier Requirements

The Group considers People Risk as: The risk that the Group fails to provide a high-performing, customer centric culture, with engaged, future focused colleagues.

| Requirement | Description |
|---|---|
| Purpose | This chapter defines the Group's expectations for external suppliers in managing their people risks and requires that external suppliers ensure that their people-related policies and processes are effective and monitored to ensure compliance with relevant legal and regulatory requirements. |
| Applicability | This chapter is applicable to all external suppliers and self-employed contractors in the course of providing services for, or on behalf of the Group. It applies specifically to, external suppliers who provide services or assign employees and self-employed contractors who will have contact with the Group's customers and/or access to:<br>• Premises<br>• Colleagues<br>• Group systems<br>• Customer or colleague data<br>Group data, including Highly Confidential/Confidential data e.g. financial reporting Management Information related to results, marketing briefs etc |
| Scope | The requirements of this chapter should be read in conjunction with the Code of Supplier Responsibility which sets out the key social, ethical and environmental values that we expect suppliers to abide by.<br>Expectations and requirements for external suppliers assigning people and/or self-employed contractors who are undertaking roles within the Group which are in scope of the Financial Conduct Authority (FCA)/Prudential Regulation Authority (PRA) regulatory Conduct Regime are included within the external supplier requirements outlined in the Group Colleague Conduct Risk Policy chapter. |
| Adherence to legislation and regulations | External suppliers must comply with all relevant legislation, regulations and directives:<br>• External suppliers operating outside the UK must comply with all UK legislative, regulatory and policy requirements set out in this document, as a minimum standard, in addition to any applicable local legal or regulatory requirements.<br>• Where local legal or regulatory requirements exceed the UK requirements set out in this document, external suppliers must comply with the higher standard.<br>• Where local legal or regulatory requirements are less stringent than the UK requirements set out in this document, external suppliers must continue to comply with the UK requirements in full.<br>• Where external suppliers are unable to meet a requirement, they must notify their Supplier Manager without delay. The Supplier Manager must engage the Policy Owner to agree an alternative compliant approach. |
| Responsible and ethical use of AI | Where external suppliers use automated systems or emerging technologies (including artificial intelligence) in the delivery of services which may impact people risk, external suppliers must ensure any associated people related risks are identified, assessed, and effectively managed, in line with Lloyds Banking Group requirements. |

| | |
|---|---|
| | External suppliers must ensure that any AI usage in services provided to LBG comply at all times with all applicable laws, regulations and regulatory requirements related to artificial intelligence in the jurisdiction(s) relevant to the external supplier and LBG. |
| Vetting | Vetting aims to safeguard the Group's integrity, security, and reputation by verifying the identity, right to work and experience of individuals, ensuring they meet our high standards.<br>• External suppliers must vet any people they assign to work for or on behalf of the Group in accordance with Group expectations. External suppliers must ensure that satisfactory checks are undertaken prior to an individual commencing work with the Group in accordance with the requirements of the Group's External Supplier Vetting Standards. These Standards will be made available to the external supplier by the Supplier Manager.<br>• External suppliers must manage any failures and/or identified issues related to individuals in a manner consistent with the Group's expectations. Suppliers must ensure that any issues identified are escalated to their Supplier Manager as soon as practically possible and a resolution agreed before the individual can be assigned to a role within the Group. |
| Human Rights | We expect all our External suppliers to respect the human rights of their own workforce, supply chain and customers, complying with all relevant legislation, regulations and directives. External suppliers must have a documented statement and/or related policies which:<br>• Prohibit forced labour (slavery) and human trafficking in their own operations and any supply chain and give all employees the right and ability to leave employment if they choose.<br>• Prohibit child labour in their own operations and any supply chain. |
| Policy and procedures | Appropriate policy and procedures aim to ensure that suppliers adhere to legal and regulatory requirements. These policies must be clear, consistent, and made available by the supplier to all individuals they assign to provide services for or on behalf of the Group:<br>• External suppliers must implement and maintain employment policies and procedures which are legally compliant, meet any regulatory requirements and show an understanding of the differing needs of a diverse workforce as outlined in The Code of Supplier Responsibility.<br>• As a minimum, policies and procedures must set out a documented approach to diversity, equity and inclusion (DE&I), performance management, disciplinary matters, grievance and harassment, including sexual harassment. They must clearly explain how individuals will be managed fairly and consistently, ensure that performance and *conduct issues are dealt with promptly, and include explicit safeguards to protect individuals from retaliation, victimisation or adverse treatment when raising concerns in good faith.<br>• Policies and procedures must include confidential reporting mechanisms, clear investigation processes and routes to additional support.<br>• Policies and procedures must be appropriately reviewed and approved, with evidence that they comply with relevant legal and regulatory requirements. |
| Training | External suppliers must ensure that any individuals they assign to the Group receive the necessary training and information to understand the key expectations of them in role.<br>External suppliers must evidence that individuals:<br>• Have the necessary capabilities to undertake that role,<br>• Understand the responsibilities and requirements of their role, |

| | |
|---|---|
| | Note - Where assigned individuals work under direct Group supervision, the external supplier must ensure that all necessary and mandatory training required by the Group is completed within the timescales stipulated. This will normally be no later than 8 weeks from the commencement of their assignment to the Group and regularly thereafter.<br><br>Where assigned individuals are not under direct Group supervision, the external supplier must monitor, record and evidence all training completion. |
| Supplier Oversight and Assurance | External suppliers remain responsible for ensuring that required people standards are met for all individuals assigned to work for, or on behalf of, the Group. They must provide supporting information and evidence when requested and promptly escalate any performance, competence or conduct issues to the Group.<br><br>Where assigned individuals are not under direct Group supervision, external suppliers must also operate appropriate supervision, monitoring, quality assurance and conduct oversight, with evidence available to the Group on request. |

# 21. REGULATORY COMPLIANCE RISK POLICY REQUIREMENTS

The risk arising from failure to follow (specific) rules, regulations and laws (including codes of practice) that apply to all stages of the customer and product journeys and managing our relationship with our regulators.

| Requirement | Description |
|---|---|
| Purpose | This Policy sets out the regulatory compliance requirements that suppliers must adhere to when providing services to, or on behalf of, the Group, ensuring compliance with applicable laws, regulations, regulatory permissions, voluntary codes, and associated standards. |
| Applicability | This Policy applies to suppliers and other third parties that undertake regulated activities for, or on behalf of, the Group, or whose services may impact the Group's ability to meet its regulatory obligations. |
| Scope | This Policy covers supplier activities that may give rise to regulatory compliance risk, including compliance with applicable laws and regulations, maintenance of regulatory permissions and licences, regulatory engagement undertaken on behalf of the Group, regulatory reporting obligations, and the management of compliance breaches and regulatory issues. It also applies to any subcontractors used in the delivery of services to the Group. |
| Due Diligence | Perform appropriate and proportionate due diligence on your sub - contractors before onboarding them and on an ongoing basis. |
| Compliance with Regulations | Identify, assess, manage and comply with all applicable local and international laws and regulations. |
| Regulatory Permissions | Identify, secure and maintain all regulatory permissions required to perform the service(s) that they are providing to, or on behalf of, the Group. |
| Systems and Controls | Put in place and maintain systems and controls to deliver against the purpose and expectations of any applicable laws and regulations. |
| Compliance Training | Provide proportionate and relevant compliance training to staff. |
| Compliance Monitoring Plan | Have a compliance plan in place to monitor, test and report on those systems and controls. For example, this might involve a log or schedule that details the regulation(s), the controls that apply and the operational effectiveness of each control. |
| Completion and tracking of remedial activity | Put in place appropriate remedial actions as required. |
| Compliance Breaches | Report any compliance breaches promptly and escalate to the Group. |
| Record Keeping | Record the relevant legal entity or Business Unit/Group Function that the activities are in support of. |
| Fourth Party Compliance | Ensure that any fourth parties (an entity that is contracted by an external supplier to deliver services or products) comply with the above requirements. |

# 22. REMUNERATION POLICY SUMMARY FOR EXTERNAL SUPPLIERS

| Requirement | Description |
|---|---|
| Purpose | The purpose of this policy is to set out what is expected from external suppliers' remuneration arrangements.<br><br>LBG is an accredited Living Wage employer. All external suppliers must adhere to the requirements of Lloyds Banking Group's Real Living Wage employer accreditation, extending fair pay to regularly contracted staff, including those employed by third parties.<br><br>External suppliers must ensure that their remuneration arrangements are designed, implemented and embedded effectively and in line with regulatory requirements, so that they lead to good customer outcomes, avoiding incentives that could lead to customer harm.<br><br>LBG is aware that its remuneration strategy and practices ultimately impact on our customers through the way we reward our colleagues.<br><br>Therefore, the Policy is fully aligned with the Consumer Duty rules and fully supports the implementation of the Group Customer Policy by ensuring that incentive structures are designed to promote good outcomes for customers and do not contain features that would encourage negative behaviours that could result in customer harm.<br><br>This policy ensures that the Group's third-party suppliers are rewarding their employees including sub-contractors in a way that encourages the right behaviours and generates good outcomes for the Group's customers. It ensures that they do not reward or assess an employee's performance in a way that conflicts with their duty to act in the best interest of the Group's customers or provides an incentive for recommending or selling a particular financial product when another may better meet the customer's needs.<br><br>This policy aligns with:<br><br>• the FCA Remuneration handbook, particularly FCA Remuneration Code (SYSC 19F) - implementing MiFID II requirements on staff incentives and the remuneration of sales staff and advisers.<br><br>• the PRA rulebook (Remuneration Instrument 2015 (PRA 2015/53)),<br><br>• FCA guidance (FG18/2) published in March 2018<br><br>• the new Consumer Duty rules (PS22/9) – ensuring fair value and good outcomes for customers. |
| Applicability | The Third-Party Supplier Remuneration Policy applies to ALL suppliers.<br><br>It is expected that all third-party suppliers will adhere to the requirements of the Living Wage Foundation.<br><br>There are additional expectations for those suppliers who reward their employees, including sub-contractors with any form of variable award in addition to base pay (e.g. bonus, commission, incentive or recognition payments).<br><br>If clarification is required, then contact your supplier manager at the Group. |
| Scope | In this policy 'Third Party Supplier' refers to any external third-party companies, organisations or partnerships that provide goods and services to the Group and/or our customers on the Group's behalf.<br><br>In addition to our own employees, regularly contracted staff, including those employed by third parties, are expected to be paid the real Living Wage as a minimum. Regularly contracted staff in this context are defined as contracted |

| | |
|---|---|
| | staff who work for the group for 2 or more hours a week, for 8 or more consecutive weeks a year.<br><br>Suppliers defined as having customer contact include:<br><br>• Those with regular and / or substantive contact with the Group's customers, e.g. via calls, face to face or direct individual emails;<br><br>• Tied Agents: offering Lloyds Banking Group specific services or products to the Group's customers, e.g. mortgages;<br><br>• Those who complete transactions, provide advice, sales or services which involves contact with the Group's customers, e.g. debt collection services, insurance claims handling, administrative services or selling of financial products;<br><br>Out of Scope<br><br>The real Living Wage does not apply to contractors that only supply products to the group e.g. stationary suppliers.<br><br>Suppliers who don't offer a variable reward to their employees do not have to adhere to the additional expectations of this policy but are still expected to pay the real Living Wage. |
| Policy Requirements | **Real Living Wage**<br><br>In addition to our own employees, regularly contracted staff, including those employed by third parties, are expected to be paid the real Living Wage as a minimum. Regularly contracted staff in this context are defined by the Living Wage Foundation as contracted staff who work for the group for 2 or more hours a week, for 8 or more consecutive weeks a year. The real Living Wage does not apply to contractors that only supply products to the group e.g. stationary suppliers.<br><br>**Third Party Remuneration Principles**<br><br>Third party remuneration policies must NOT incentivise behaviours that prioritise personal or supplier interests, over the best interests of the Group's customers.<br><br>Base pay must not be delayed or reduced if performance targets linked to variable awards are not met.<br><br>Suppliers may operate several variable reward plans tailored to different roles or teams. However, these must align with the Group's own risk appetite and guidance issued by the Financial Conduct Authority.<br><br>**Incentive / Variable Plan Structure**<br><br>• Balanced Remuneration: Fixed pay should form a substantial portion of total remuneration—ideally at least 70%—to avoid over-reliance on variable pay. Exceptions should be limited to exceptional performers or where market norms justify it.<br><br>• Manager Incentives: Managers' incentives should be based on different metrics than their teams to prevent undue pressure and ensure fair treatment of customers.<br><br>• Proportional Rewards: Incentive schemes must avoid disproportionate rewards for marginal transactions, such as:<br><br>  ○ Single transactions significantly impacting awards<br><br>  ○ All-or-nothing thresholds<br><br>  ○ Accelerators or stepped payments<br><br>  ○ Cliff-edge performance targets that may compromise service quality |

- Product Neutrality: Campaigns or promotions must not favour one product over another.

**Performance Metrics**

- Performance must not be solely based on sales targets such as volume, profitability, or productivity (e.g. number of products sold, calls handled, and cases administered).
- Performance metrics must include quality metrics that promote and ensure right behaviours and better customer outcomes (e.g. call monitoring, cancellation rates and customer feedback).
- Performance metrics must not encourage the sale of one product being preferred over another (i.e. product bias).
- Risk factors must be considered when an award is determined, e.g. complaints, customer service levels or not following due process.

**Management Information**

- MI should be scrutinised regularly with performance and spend tracked to ensure the plan is awarding as expected. Regular (or significant) under and over performers should be assessed to ensure good customer outcomes are maintained, e.g. under performers are recognised and provided additional support or the results of high performers are reviewed to ensure that they are based on good customer outcomes.

**Business Quality Monitoring**

- Ensure a customer focus: employees should be encouraged to prioritise excellent customer service and advocacy.

**Deferral / Claw back**

- Deferral or claw back arrangements must be linked to appropriate measures and are carefully monitored.
- Salary should not be delayed or reduced due to unmet objectives.
- Substantial salary increases should only occur through formal processes (e.g. promotions), not for meeting performance objectives.

**Controls**

- Third party suppliers must evidence that they comply with the Living Foundations real Living Wage rates of base pay for all their employees regularly contracted to work for the Group.
- Third party suppliers should ensure that they take reasonable care to organise and control their affairs responsibly, effectively and with adequate risk management systems.
- The types of controls and governance a third-party supplier must have in place should reflect the nature, scale and complexity of its business and the risk its activities may pose to the Group's customers.
- Third party suppliers should consider how incentives or performance management might cause, or increase, the risk that they may not comply with recommended guidance, this must be determined through the completion of the customer outcome questions.
- Third party suppliers should satisfy themselves that staff are following processes and that they are leading to good customer outcomes. This could be evidenced through appropriate management information which helps identify potential indicators of risk and/or business quality monitoring.
- A senior policy owner at a third-party supplier must review and approve their incentive schemes, at least annually to ensure it remains fit for purpose and in line with risk appetite and market practice.

| | |
|---|---|
| | • Third party employees should receive annual communication on how their variable reward operates, and how customer service and risk factors can impact their award.<br><br>**Terminology Clarification**<br><br>• To avoid confusion, the Group defines the key terms as follows:<br><br>• Bonus plans: typically awarded at the end of the financial year based on annual individual, business or overall company / group performance;<br><br>• Commission / Incentive plans: arrangements where the level of an employee's award is directly influenced by performance against individual metrics including, but not limited to sales, revenue or productivity targets;<br><br>• Recognition plans: An award made in recognition of individual performance that exceeds £500 in a financial year;<br><br>• Salary adjustments: a change to an employee's contractual fixed pay outside of the usual pay / promotion process. |
| Compliance | In line with the Group's criticality assessment approach, suppliers with a criticality assessment outcome of Super Severe, or Severe, have assurance assessments carried out between 1- and 3-years dependent on risk factors.<br><br>**Non-Compliance**<br><br>Any material differences between the requirements set out above and the supplier's own variable pay arrangements should be raised with the supplier by the Group's Supplier Manager who will then discuss the non-compliance with the Accountable Executive for the relationship, the Reward function within the Group's People and Places team and the local Risk team to agree a way forward. |
| Appendices | Link to the Living Wage Foundation website. |

# 23. SANCTIONS RISK POLICY REQUIREMENTS

These requirements must be followed to manage the risk that the Group makes funds or economic resources available directly or indirectly, to a sanctioned country / region, individual or entity or makes payments / undertakes trade which involves sanctioned goods / services, in contravention of domestic or international regulations or legislation.

| Requirement | Description |
|---|---|
| Purpose | The purpose of this policy is to establish the minimum sanctions and export control requirements applicable to external suppliers providing goods or services to, or on behalf of LBG. It defines the standards and parameters which must be followed to manage Economic Crime Risk within Board approved risk appetite and enable compliance with all applicable regulation, legislation and associated standards that the Group must adhere to.<br><br>The Group Economic Crime Prevention Risk Policy defines the minimum global requirements for managing economic crime risks, primarily informed by UK regulatory expectations. It is designed to ensure that LBG does not knowingly establish or maintain relationships with third parties, that could expose LBG to sanctions breaches, sanctions evasion, regulatory action, financial loss or reputational damage. No individual within the Group, or acting on its behalf may undermine or circumvent the intent of this policy<br><br>This summary sets out how the Economic Crime Prevention Policy (Sanctions) requirements apply to External Suppliers. |
| Applicability | These policy requirements apply to external suppliers where it has been determined that the Sanctions Risk Policy is applicable to the services they provide to, for, or on behalf of the Group.<br><br>In jurisdictions where the local legislative and regulatory requirements exceed the requirements set out in this document, the Supplier must comply with any higher standards. |
| Scope | An external party supplying services to the Group or performing services on the Group's behalf will be expected to comply with the Group's Economic Crime Prevention Policy (Sanctions) where those services form part of the Group's regulated activities.<br><br>In all other circumstances, this Policy is not applicable to external suppliers of goods or services to the Group.<br><br>Typical circumstances that will result in the Sanctions requirements of the Economic Crime Prevention Policy being applicable include the following services:<br><br>• On-boarding or introducing customers;<br>• Payment or transaction processing;<br>• Regulated products or services and;<br>• Providing risk, compliance or audit services to the Group.<br><br>Typical circumstances that will not result in the Sanctions requirements of the Economic Crime Prevention Policy being applicable include:<br><br>• Providing goods to the Group; and<br>• Performing services unrelated to the Group's regulated activities (e.g. security, transport, catering, printing, etc.);<br><br>LBG reserves the right to apply this policy to any supplier where the inherent sanctions risk warrants additional controls. |

| | |
|---|---|
| Dealing with Prohibited Countries & Geographical Regions | The Group will not maintain any relationships, process payments to or from (directly or indirectly), or undertake commercial transactions with entities or individuals based in the countries listed below. This prohibition applies to all transactions and payments in all currencies:<br>• North Korea<br>In addition to the above, certain restrictions and prohibitions apply when dealing with Syria, Iran, Cuba, Belarus, Russia, the non-Government controlled regions of Ukraine; Luhansk, Donetsk, Kherson, Zaporizhzhia, and the Crimean Peninsula (including Sevastopol).<br>Therefore, we require in scope suppliers to the Group to ensure they do not deal with any of these countries on behalf of the Group without prior agreement.<br>Suppliers must ensure that they meet all UK, and UN Sanctions obligations.<br>In addition, EU and US Sanctions obligations must be applied when there is an EU or US nexus to the supplier or any associated transaction.<br>**EU nexus:**<br>• The supplier or any party associated with the activity are incorporated or constituted under the law of an EU Member State.<br>• The activity is conducted at least partly within the EU, even if the parties involved are non-EU persons or entities<br>**US Nexus**<br>• Involvement of US Persons:<br>1. All US citizens and permanent residents, regardless of where they are located.<br>2. All individuals and entities within the United States.<br>3. All US incorporated entities and their foreign branches.<br>• Use of US Financial System:<br>1. Transactions that pass-through US banks, even if the parties are non-US persons.<br>2. Use of US dollars in international transactions often triggers US jurisdiction due to clearing through US financial institutions. |
| Due Diligence | The Supplier must complete risk-based Sanctions due diligence on persons (including individuals and incorporated and unincorporated bodies) who will perform services for or on behalf of the Group which is appropriate and relevant to such services.<br>In determining whether a person is acting for or on behalf of the Group, the Supplier must consider the nature of the activity being undertaken. As a minimum, an agent, subsidiary or any other person obtaining, retaining or conducting business on behalf of the Group must be subject to due diligence. |
| Screening | The Supplier must have procedures for screening transactions, individuals, entities and employees against relevant sanctions lists:<br>• UK Sanctions List<br>• OFSI restricted List<br>• OFAC Specially Designated Nationals and Blocked Persons List<br>• OFAC Consolidated Sanctions List (Non-SDN Lists)<br>• EU Consolidated List |

| | |
|---|---|
| | • EU Financial Restrictions List |
| Conduct | In order to ensure the effective implementation of Sanctions and the traceability of funds connected with terrorist financing, it is essential that the Group is not knowingly involved; in attempts to frustrate or circumvent the Sanctions regime of any country or regional body. Activities which are expressly forbidden, may include but are not limited to:<br>• Omitting, deleting or altering information in payment messages for the purpose of avoiding detection of that information by other financial institutions in the payment process.<br>• Using a particular payment messaging system for the purposes of avoiding detection of that information within the Group and/or other financial institutions in the payment chain; and<br>• Encouraging or providing guidance to customers and suppliers on circumventing any Sanctions prohibitions or restrictions.<br>• In addition, procedures must be in place to inform the Group if the Supplier breaches financial and trade sanctions regulatory requirements. |
| Training | The supplier must ensure all employees / contractors complete Sanctions training no later than 8 weeks from the commencement of their employment and annually thereafter to understand how the requirements of relevant sanctions legislation and this Policy Summary affect their role and individual responsibilities.<br>Where employees are identified as working in roles considered high risk for Sanctions, role specific training must be considered to ensure that employees are aware as to the increased sanctions risks associated with their roles. |
| Management MI | External Suppliers must ensure that MI is produced that includes details on the levels of compliance in relation to:<br>• Training;<br>• Number of actual or suspected breaches of financial and trade sanctions reports raised;<br>• Record keeping.<br>MI must also identify where remedial action is required.<br>The External Supplier must ensure that Governance arrangements are in place that ensure the escalation of MI and results of oversight and monitoring programme to the External Suppliers Senior Management and LBG (as agreed) allowing for the effective management of Sanctions risks in a timely manner. |
| Non-Compliance | Any material differences between the requirements set out above and the supplier's own controls must be raised by the Supplier with Lloyds Banking Group's Supplier Manager.<br>The Supplier Manager will then discuss the non-compliance with the Accountable Executive for the relationship and local Risk team to agree way forward. |

# 24. Speak Up Policy Summary for External Suppliers

The risk that the Group does not manage concerns raised through whistleblowing and other reporting routes which adversely impacts customers, colleagues or business operations.

| Requirement | Description |
|---|---|
| Purpose | Lloyds Banking Group expects its external suppliers to promote a culture where all individuals working for or on behalf of the supplier (referred to in this chapter as 'colleagues') feel comfortable to openly raise concerns.<br><br>This policy supports suppliers to embed whistleblowing arrangements and a speak up culture. It also details how to report or escalate concerns directly to Lloyds Banking Group. |
| Applicability | Suppliers operating outside the UK must ensure that local country and jurisdictional legislation and regulatory requirements are adopted in addition to the requirements below.<br><br>Local laws or regulations must take precedence. As such, where these laws or rules conflict with, or result in, any requirements not being fulfilled, or where any of the requirements prohibit an activity that is mandatory under local law, the external supplier must inform Lloyds Banking Group to agree what actions should be taken. |
| Scope | This policy applies to all suppliers providing services to or on behalf of Lloyds Banking Group.<br><br>Lloyds Banking Group's Speak Up framework accepts reports made by a broad range of individuals, including (but not limited to):<br><br>• current or former employees<br>• agency workers, temporary staff, secondees, trainees, volunteers and job applicants<br>• contractors and subcontractors, consultants, suppliers and their employees<br>• directors, officers, board members and shareholders<br><br>A Speak Up concern will involve some form of actual or suspected wrongdoing or misconduct that may pose a risk to customers, colleagues, Lloyds Banking Group, or the wider public. |
| Ensuring Unrestricted Reporting | Suppliers must make sure there are no obstacles or attempts to prevent colleagues from reporting a concern including via contracts of employment, settlement agreements, non-disclosure agreements and confidentiality agreements.<br><br>Suppliers must not require colleagues to provide evidence when raising a concern but may require colleagues to have reasonable belief that the information provided is true. |
| Policy & Procedures | Suppliers are required to have a policy and/or procedures detailing their whistleblowing arrangements, which must include the following key points:<br><br>• Colleagues are encouraged to speak up if they suspect or witness wrongdoing.<br>• Examples of wrongdoing relevant to the supplier's area of business. For example, this may include (although this is not an exhaustive list):<br>  ○ Failure to comply with law, regulations, policies, procedures, or customer treatment standards<br>  ○ Inappropriate or unethical behaviour including any form of discrimination, harassment (including sexual harassment) or |

| | |
|---|---|
| | victimisation of, or retaliation against, any individual for raising a concern<br>○ Criminal activity such as theft, fraud, financial crime, bribery and corruption, or modern slavery/labour exploitation<br>○ Actions or conditions that pose a risk to colleague or public safety<br>○ Damage to the environment or concerns about misleading customers or shareholders (e.g. 'greenwashing')<br>○ Data protection breaches or cybersecurity incidents<br>○ Other risks or malpractice that might impact customers, colleagues, the supplier's business or clients (including Lloyds Banking Group)<br>○ Any attempts to hide, destroy or alter information relating to any of the issues listed above<br>• Details of clear and accessible internal reporting route(s) available to colleagues to report suspected wrongdoing within the supplier's organisation.<br>• Assurance that all concerns reported will be treated seriously and in a confidential manner.<br>• A statement that management inaction is not tolerated and may be subject to formal action under the supplier's applicable disciplinary process.<br>• A statement that retaliation against any colleague reporting a concern is not tolerated and may be subject to formal action under the supplier's applicable disciplinary process. |
| External Reporting Routes / Independent Advice | In case colleagues do not feel comfortable reporting their concerns to their management/organisation, external supplier colleagues working on/related to the Lloyds Banking Group contract must be made aware how they can a) report externally (which includes directly to Lloyds Banking Group) and b) seek external, independent advice. These routes are:<br>• Online or by telephone to Lloyds Banking Group's Speak Up Service<br>○ https://lbgspeakup.ethicspoint.com<br>○ Phone: +44 (0)800 0141 053 (suppliers based outside of the United Kingdom may signpost the relevant local telephone number which can be found at the URL above)<br>• By email directly to Lloyds Banking Group Speak Up team<br>○ Email: speakup@lloydsbanking.com<br>• Externally to the UK Financial Service Regulators<br>○ Financial Conduct Authority:<br>○ Email: whistle@fca.org.uk<br>○ Phone: +44(0)207 066 9200<br>○ Prudential Regulation Authority:<br>○ Email: whistleblowing@bankofengland.co.uk<br>○ Phone: +44(0) 203 461 8703<br>External supplier colleagues can seek external confidential advice or independent legal advice from the UK Whistleblowing charity, Protect. Protect can discuss options and help them raise a concern about wrongdoing at work. Colleagues do not need to be located in the UK to use this service, and interpreters are available if required.<br>○ Online: protect-advice.org.uk |

| | |
|---|---|
| | ○ UK Freephone: 020 3117 2520 |
| Responding to a concern | All concerns raised within the supplier organisation must be dealt with confidentially, and supplier colleagues must be offered protection in respect of the information provided wherever possible and in accordance with local law/regulation.<br><br>Supplier management must notify Lloyds Banking Group as soon as possible upon becoming aware of any Speak Up/whistleblowing concerns relevant to Lloyds Banking Group. Typically, this should be done through the Lloyds Banking Group Supplier Manager; however, if there is a conflict of interest or other reason, concerns may be reported directly using the channels listed under the External Reporting Routes section.<br><br>If a supplier is required to conduct an investigation that affects Lloyds Banking Group or its customers, the supplier must make sure that:<br><br>• Competent and appropriate resources are available for dealing with the investigation<br><br>• The investigation is conducted independently, with any potential or actual conflicts of interest managed appropriately<br><br>Where the supplier's investigation of a Speak Up concern identifies a weakness in the supplier's controls or processes that has a customer, regulatory or financial impact on Lloyds Banking Group, this must be reported to Lloyds Banking Group as soon as possible.<br><br>In the case that Lloyds Banking Group initiates an investigation involving the supplier or its colleagues, supplier colleagues and management must assist Lloyds Banking Group with its enquiries. |
| Training & Awareness | Supplier management must communicate the following to all colleagues supporting a Lloyds Banking Group contract within 8 weeks from the commencement of their employment or the contract with Lloyds, and annually thereafter.<br><br>• A statement encouraging colleagues to Speak Up if they suspect or witness wrongdoing<br><br>• A commitment that concerns will be taken seriously, treated confidentially and with zero-tolerance for retaliation<br><br>• Examples of concerns that can be raised<br><br>• Available internal reporting routes within the supplier's management/organisation<br><br>• Available external reporting which includes directly to Lloyds Banking Group's Speak Up service and relevant Regulators<br><br>• Sources of available support (e.g. Protect) |
| Record-Keeping | Suppliers must maintain accurate and adequate records of:<br><br>• Reports received<br><br>• Investigations conducted<br><br>• Actions taken<br><br>• Induction and annual training/communication provided to colleagues<br><br>Records must be preserved in accordance with applicable laws and be made available to Lloyds Banking Group upon legitimate request. |

## UPDATES TO EXTERNAL SUPPLIER POLICIES

| Update Type | Approach |
|---|---|
| Scheduled | A review of all policy requirements will be performed in Q1 annually. |
| Triggered | Out of cycle reviews may be triggered to accommodate material change requirements, including changes to regulatory expectations. |

## VERSION CONTROL

| Version | Date | Summary of Change | Status / Notes |
|---|---|---|---|
| 1.0 | T.B.C | First iteration of the consolidated single document for external supplier policy requirements. | This version brings together supplier-facing requirements into one consolidated document. Most included policies already existed as standalone supplier policies or had requirements captured under other policy documents. The only completely new policy areas included for consideration are Model Risk, Client Assets and Financial Reporting & Tax. |