TSB Policy Summaries

This document provides potential TSB suppliers with the principles and objectives of each policy which TSB deem to be important when dealing with suppliers. The document also includes controls that TSB has internally to ensure that any potential supplier adheres to these policies.

Name of Policy	Anti-Money Laundering, Anti-Bribery and Corruption and Sanctions Policies.

Objective:

TSB's Financial Crime framework is supported and reinforced by our Behaviours, which puts the customer at the heart of everything we do. Compliance with our Financial Crime framework is a key demonstration of our Behaviours to ensure TSB operates responsibly, transparently and with integrity. TSB has a moral, legal and regulatory duty to prevent, detect and deter financial crime. We care about our customers and Partners, and the communities we serve, and strive to protect them from those who would try to use TSB to commit financial crimes.

Controls:

TSB's Anti-Money Laundering and Counter-Terrorism Financing programme

To facilitate compliance with anti-money laundering (AML) and counter terrorism financing (CTF) laws, TSB has developed and implemented an AML and CTF programme consisting of an AML & CTF Policy, procedures, internal systems and controls and monitoring and assurance. To comply with AML and CTF laws and regulations, TSB's AML & CTF Policy and mandatory requirements includes:

- Customer risk assessment.
- Customer due diligence measures driven by customer type.
- The identification and, where necessary, verification of beneficial owners.
- The identification and risk assessment of Politically Exposed Persons.

Enhanced due diligence for all high-risk clients, including source of funds, source of wealth, adverse press:

- Periodic ongoing reviews driven by customer risk.
- Event driven triggers to ensure customer due diligence remains up to date and reflective of any risks posed within relationships.
- Automated monitoring of transactions to identify patterns of suspicious activity.
- Internal procedures for monitoring and reporting suspicious activities.
- The appointment of a Nominated Officer and relevant procedures for reporting suspicious activities to the designated Financial Intelligence Unit.
- The appointment of a MLRO, who has overall responsibility for ensuring TSB's compliance with relevant financial crime legal and regulatory requirements.
- The retention of relevant records in line with TSB's regulatory obligations and internal policy requirements.
- The provision of advice and management reports to senior management regarding compliance with AML and CTF laws and regulations.
- Regular staff training and awareness, appropriate to the role, including training of senior management.
- The promotion of effective compliance through a range of independent assurance testing and audit activity to provide appropriate oversight and follow-up actions in the event of non-compliance.
- The management of regulatory enquiries and incidents.

TSB's Sanctions and Related Prohibitions programme

TSB has a Financial Sanctions Policy and mandatory requirements in place designed to comply with its obligations under UN and UK sanctions regimes. Consideration is also given to EU and US sanctions, due to TSB's ownership by and correspondent banking relationship with Banco de Sabadell, S.A. TSB takes a prohibitive stance towards transactions and customer relationships involved in countries subject to comprehensive international financial sanctions or owned or controlled by persons located in such countries. Partners, customers, suppliers and payments are screened regularly against relevant sanctions lists and investigated accordingly. Any TSB relationship identified as a designated person/entity is frozen and reported, internally and externally, in accordance with the applicable regulations.

TSB's Anti-Bribery and Corruption programme

TSB has no appetite for breaching anti-bribery and corruption legislation and regulation. This includes activities conducted by any 'associated persons' supplying goods or services for TSB, intermediaries or brokers introducing business to TSB, as well as those otherwise acting on TSB's behalf. TSB's Policy applies to all Partners, whether on a permanent, fixed or temporary contract, and all contractors and agency staff across all business areas and all interns or work experience persons. To comply with relevant laws and regulations we:

- Have clear and specific Senior Management responsibilities and accountabilities.
- Issue internal communications to convey the 'tone from the top'.
- Ensure adequate and competent resource is available.
- Provide Partners with training so they are aware of their responsibilities.
- Conduct risk assessments to understand the risks we face and establish an appropriate control framework to manage those risks.
- Identify, assess and monitor emerging risks and manage these in line with our risk appetite.
- Have adequate anti-bribery and corruption policies and procedures in place which are proportionate to the level of risk exposure.
- Have a Gifts, Entertainment and Hospitality Policy* that outlines the requirements that must be followed.
- Monitor our procedures, systems and controls to ensure they are operating effectively.
- Escalate breaches and any material or significant events and act to address any weaknesses in our controls.
- Conduct due diligence on all third-party relationships entered into and on an ongoing basis.
- Have a Whistleblowing Policy* to support Partners who feel unable to report through their line manager. Under TSB's

- Anti-Bribery and Corruption Policy, the following activities are fully prohibited:
- Facilitation payments.
- Political donations.
- Facilitation of tax evasion.

*Policies managed out-with the Financial Crime framework however which are relevant to the management of ABC risks

Additional Information:

TSB's compliance with financial crime policies and technical standards is monitored via several methods, including control testing; oversight and assurance; audit and the provision of management information and oversight by senior governance committees.

Specific control requirements will depend upon the nature of the service or function being performed and will be confirmed to the Supplier by TSB's contracting party.

Any material differences between the requirements set out above and the supplier's own controls should be raised with TSB.

Name of Policy	Change Policy

Objective:

At TSB, we care about our customers and colleagues. As a result, the Change Policy is in place to mitigate the risk of any negative customer impact, supporting our regulatory expectations of acting to deliver good outcomes for our customers, additional cost, or reputational damage which may arise from change initiatives failing to deliver.

This Policy applies to both Investment and Non-Investment change. Within this there are five recognised "types" of change (detailed below). The degree to which change is required to comply with the underpinning technical standards and governance will vary dependent on the category and nature of the change being progressed.

- Project Change (this includes Discretionary and Legal, Regulatory, and Mandatory (LRM) change projects that will be delivered to achieve a business objective).
- Project Change is usually complex and will typically have an impact on the TSB business, (it may be grouped into Programmes to align to wider delivery).
- Project Change will normally require the mobilisation of resources to deliver and can take a significant time to be implemented.
- Project Change can be differentiated between Large, Medium and Small Projects. Delivery cost is the primary measure to support this categorisation; (Large Projects ≥ £1m, Medium projects ≥ £100k & < £1m and Small Projects < £100k).
- Large and Medium sized projects are required to fully comply with the Change Standards and to also follow the full end to end Delivery Lifecycle. Where exceptions to the standards are required, these should be raised by the Project Manager for approval.
- Small Projects would be expected to have no/limited impact on either the business or technical operating model. Small projects are not mandated to follow the full end-to-end Delivery Lifecycle, however, where these changes impact Production environments, they are controlled through compliance with the Bank's IT Certification and IT Change Approval guidelines.

- The Evolve programme is creating a new Agile way of working. This will ultimately require updates to the Change Policy and Change Standards (expected in 2024) to cover the creation of a new SDLC, and associated accountabilities and operating model. Meanwhile, projects working within the Evolve "Glass Tube" are covered under Waiver 735.
- Keeping the Light on Services (KTLO): Regular business configuration or reporting activities which are defined in the Service Catalogue. These are managed directly between the relevant business function and their IT Supply lines.

The majority of KTLO effort does not change production environments and is focussed on regular required maintenance (eg health checks, monitoring of batch runs and applications and incident resolution). In some cases lower risk changes are required by KTLO and where these changes impact Production environments, they are controlled through compliance with the Bank's IT Certification and IT Change Approval guidelines (please refer to the Change Standard for further information). This ensures no change is brought into production without appropriate QA, assessment, visibility and approval

- Maintenance Change is defined as on-going systems, network, infrastructure, or software changes, including upgrades, performance enhancements and modification or patching. This type of change is generally invisible to customers and colleagues and will be managed directly by the CIO function. Where these changes impact Production environments, they are controlled through compliance with the Bank's IT Certification and IT Change Approval guidelines. However, a set of standards is being formalised following findings from the recent "Technical Assurance in Change Delivery" audit to ensure that there is appropriate QA, assessment, visibility and approval.
- Factory Change is intended to be self-contained within each factory where possible, utilising fixed capacity teams to deliver discrete projects of small/medium size. Factory Change must follow the defined Factory Change framework (a simplified view of the end-to-end Delivery Lifecycle, incorporating the key material governance steps required for a safe and controlled implementation).
- Non-Investment/BAU: There is no requirement for Non-Investment/BAU business change to fully comply with the Change Standard and/or follow the full end to end Delivery Lifecycle (these changes are typically smaller in nature or non technical). Project Business Accountable executives are accountable and responsible for ensuring their change is well managed, giving appropriate consideration to downstream dependencies and to ensure risks are effectively controlled to reduce/mitigate any adverse impact. As mentioned above, all changes impacting Production environments are required to comply with the Bank's IT Certification and IT Change Approval guidelines.
- Emergency Change is not a separate "category" of change. It should be viewed as an alternative deployment approach which may be required due to a rapidly changing environment or exceptional circumstances (changes may require an accelerated route to live in order to facilitate fast delivery). The IT Change Authority will provide authorisation for emergency changes which will be approved in accordance with the IT Change Management Process (please refer to the Change Standard for further information). Emergency change is not required to fully comply with the Change Standard and/or follow the full end to end Delivery Lifecycle.

- The TSB Change Policy (the "Policy") sets out:
- Who the Policy applies to and why these Colleagues will adhere to the requirements outlined, when delivering change.
- How we measure our risk appetite and Policy adherence, in line with our robust governance and testing processes for change (as detailed within the Change Standard and Testing Standard, please see below).
- What we need to pay close attention to and how to mitigate the key risks identified when delivering change.

Policy Principles

- What we must do:
- Quality Assurance Governance Framework - Carry out appropriate testing and assurance activities as appropriate for the type of change being delivered and as designed within the TSB Testing Standard.
- Risk Management - Continuously seek to identify, mitigate and manage existing delivery risks in line with TSB Operational Risk Policy and Risk Management Framework Standards.
- Budget Controls and Monitoring - Ensure all governance is in place for all financial and benefits tracking, ensuring control is maintained around change activity & budgetary spend, including third party costs.
- Governance of Delivering and Embedding Change - Ensure clear accountability for each change, it is a requirement that an Accountable Executive is always assigned. All supporting Standards will be made available to all key stakeholders and Third Parties delivering change and must be followed.
- Information and Communication Security - Record and retain all physical assets and hardware relating to the delivery or testing of change. Regular control testing must be carried out in order to ensure compliance with the Bank's Data Protection and Information Security requirements.
- Evidence that we are prioritising the resilience of the Important Business Services (IBS) as an intrinsic part of how we run our business.

Controls

- Compliance with the Bank's IT Certification and IT Change Approval guidelines (inc Release management controls)
- Testing of all Primary controls via control testing.
- Ensure all project and testing information, data and deliverables are monitored and approved as required.
- Consistency and mandatory adherence to the Change Policy/Standards when delivering "change" at TSB.
- Assessment to outline how change will impact the operational resilience of any Important Business Services and which of these will be impacted.

Additional Information

Name of Policy	Conflict of Interest

Objective:

TSB provides a range of personal and business banking products to support our customers' needs. Because of this TSB acts in a number of different capacities which can cause actual or potential conflicts of interest. TSB's Conflicts of Interest Policy supports the bank in ensuring that it complies with all regulatory and legal requirements in place from time to time regarding managing conflicts of interest.

Policy Principles:

A conflict of interest is a situation where someone (a business or an individual) has competing professional or personal interests which can make it difficult for them to fulfil their duties fairly. At the very least, a conflict of interest could create a bad impression and undermine confidence in the ability of that person to act appropriately. A conflict of interest, if not managed appropriately, poses the risk of detriment to one or more customers, or to TSB. In addition, the conflict or mere appearance of a potential conflict of interest can significantly impact TSB's brand and reputation.

TSB's Conflicts of Interest Policy is designed so that actual and potential conflicts of interest within TSB are identified, documented, managed and, where appropriate, disclosed to customers.

All persons engaged in activity on behalf of TSB must consider their day-to-day actions, identify any actual or potential conflict of interest and escalate it appropriately. Suppliers must identify where conflicts of interest may occur and have in place appropriate strategies and controls to mitigate the risks arising.

Controls:

As a minimum, all suppliers must:

- Have procedures in place, aligned with TSB's Key Principles, to identify and manage actual and potential conflicts of interest with its customers and other stakeholders (including TSB).
- Ensure their employees complete appropriate and proportionate training on the procedures in place on induction and regularly thereafter.
- Ensure that records are kept of Conflicts of Interest identified.
- Maintain appropriate MI and reporting including breach reportingAdhere to all relevant legal and regulatory requirements.
- Report to TSB a conflict or potential conflict with TSB or any of its customers, and
- Not engage in any activity which breaches TSB Policy.

Additional Information:

Any material differences between the requirements set out above and the supplier's own controls should be raised with TSB.

Name of Policy	Complaints Policy

Objective:

We care about our customers. We try to do the right thing so that our customers are treated properly by us. When we know that this hasn't happened, we'll quickly do what we can, to put it right. Put simply, we think about our customers first.

We comply with the FCA Glossary Handbook definition for a complaint and PSD complaint. The Handbook should be referred to for the full definitions, internal summary below: -

- Any oral or written expression of dissatisfaction, whether justified or not, from or on behalf of, a person or business about the provision of, or failure to provide, a financial service (including a payment service) or a redress determination, which alleges that the complainant has suffered (or may suffer) financial loss, material distress or material inconvenience.

Policy Principles

What we do

- We comply with rules and guidance regarding aiding consumer awareness.
- We establish, implement and maintain effective and transparent procedures for the reasonable and prompt recognition and handling of customer complaints.
- We comply with complaints resolution rules and guidance by;-
  - Conducting effective complaints investigations diligently and impartially, reviewing all additional information as necessary.
  - Providing a fair, consistent and prompt customer outcome and offering appropriate redress or remedial action.
  - Providing the customer with a prompt, clear and fair explanation of the assessment of the complaint and the decision made on it.
- We have in place appropriate management controls and take reasonable steps to ensure that in handling complaints we identify and remedy any recurring problems.

- We have appropriate management controls in place and take reasonable steps to ensure we identify and remedy any systemic problems, including those identified through complaints.
- We have procedures in place for third parties to make a complaint on behalf of our customers e.g. Solicitors.
- We comply with complaints time limit rules.
- We comply with complaints forwarding rules and complaints time barring rules.
- We comply with complaints record keeping requirements.
- We comply with rules relating to reporting complaints MI to the FCA.

Controls

- Training to ensure Partners understand the definition of a complaint and can recognise when a complaint should be recorded.
- TSB Learning and Competency scheme.
- Annual Mandatory Training.
- Review of FOS decisions.
- Risk Appetite Measures for Complaints.
- Complaints MI & Tracking to identify any emerging trends.
- Complaints Root Cause Analysis and robust feedback loops.
- Quality Control and Quality Assurance to monitor effectiveness and customer fair outcomes.

Additional Information

Specific control requirements will depend upon the nature of the service or function being performed and will be confirmed to the Supplier by TSB's contracting party.

Any material differences between the requirements set out above and the supplier's own controls should be raised with TSB.

Name of Policy	Data Governance & Data Quality Policy

Objective:

Data governance provides an accountability framework that ensures data is owned by the right people in the business, is clearly defined and understood, and adequately controlled so the people who use data can trust it.

The aim of this policy is to ensure we apply data governance to take an appropriate and consistent approach to the management and ownership of the risks associated with data quality for our critical data throughout its lifecycle.

The key business objectives for data governance are to:

- Provide confidence and instil trust in data to support informed decision-making, increased operational efficiency and enable innovation at pace by ensuring the right data is collected and its integrity remains intact throughout its lifecycle
- Enable compliance with regulatory and legislative requirements to maintain customer trust
- Help assess the data impact of change and reduce the likelihood of service disruption.
- Ensure consistency and reliability of services provided to customers

We do this so that the business can trust its data - to deliver the services we offer to our customers and to report our current state and performance to our management, regulators, and shareholder.

Data Governance is a core component of effective data management which also includes data protection, information security and records management.

The standards set out how we:

- Ensure business ownership of our data.
- Ensure expert partners have defined the critical data that we create, produce, procure or collect.
- Clearly state how we can tell if that data is right.
- Ensure the people that produce, transform and consume data are clear about who and how the bank ensures that it is correct.
- Define the roles and responsibilities that are required to make that possible.

This policy This policy is a key component of TSB's compliance with the European Central Bank Guide to Internal Models and Basel Committee for Banking Supervision Principles for Effective Risk Data Aggregation and Risk Reporting (BCBS239).

Policy Principles

- Accountability Framework: Embed the data governance accountability framework.
- Identify critical data elements (CDEs): Capture all critical data of the bank and its metadata and ensure ownership is agreed.
- Lineage & Source compliance: Trace the lineage of any regulatory critical data back to the authoritative data source.
- Data Aggregation Capabilities and Data Quality Incident Management: Manage the data quality across TSB's critical data to ensure the integrity of this data.
- Data Quality Management: Operation of appropriate data quality controls to maintain the integrity of the data that is used and created.
- Risk & Controls: Ensure data management controls are effective

Controls

We manage 4 centrally operated general controls to help mitigate data risks:–

- Register of Data Governance Role Holders
- Critical Data Element Glossary,
- Data Lineage and
- Data Quality Testing

Additional Information

Data Governance and Data Quality Management Policy has four associated standards:

- Data Governance Accountabilities – describes our accountability framework.
- Business Metadata – defines what we need to know about our critical data to describe it accurately.
- Data Lineage – defines how data flows through the data infrastructure so we can identify it as well as the level of governance required in the documentation process.
- Data Quality - defines our data quality management framework.

The standards describe how data quality management is integrated with the business through the ownership of data domains and how we inform our senior management of the control of the data landscape of the bank as required by regulation.

Name of Policy	Data Privacy Policy

Objective:

To assess and define that there are robust and secure controls in place to ensure that data acquired, processed, and shared between TSB and its suppliers is necessary, has a lawful basis for doing so, is controlled and there is a collaborate and timely exchange between parties if there is an identified need for improvement impacting on the ether our legislative requirements or customer treatment.

Policy Principles:

The bank and its suppliers must have appropriate technical and organisational measures to ensure that data which is acquired, processed and/or shared is done so:

- In accordance with an appropriate lawfulness for processing.
- Accurately, adequately, and proportionately.
- Securely, fairly and transparently, and
- Transferred only to parties/territories that have sufficient legal arrangements in place.

Controls:

The established controls to manage, mitigate and communicate risks are the terms of the commercial contract which set out:

- The basis and terms on which data is processed.
- The requirement for appropriate technical and organisational measures.
- The requirement for notification of incidents and breaches which may indicate control gaps.
- The requirement for suppliers to notify any changes to systems/suppliers impacting on customer data.

Additional Information:

Specific control requirements will depend upon the nature of the service or function being performed and will be confirmed to the Supplier by TSB's contracting party.

Any material differences between the requirements set out above and the supplier's own controls should be raised with TSB.

Name of Policy	Environment – Do What Matters

Objective:

Please see TSB's Do What Matters Plan for our approach and expectations for environmental impact reduction:
The Do What Matters Plan | Planet | TSB Bank

Name of Policy	Health & Safety Policy

Policy Principles:

The Bank has a duty to comply with prevailing legal and regulatory requirements. In the United Kingdom these include (amongst others):

- Health and safety at Work Act 1974.
- Regulatory Reform (Fire Safety Order) 2005.
- Fire Safety Scotland Regulations 2006.
- All subordinate health, safety and fire legislations applicable to the supplier's activities.

TSB has a framework of guidance and standards to maintain the highest health safety and fire standards through our business activities.

The Bank is committed to complying with its legal and regulatory responsibilities in relation to Health, Safety and Fire and has no tolerance for fatal incidents or serious injuries.

Suppliers must ensure they:

- Support the development, communication and implementation of effective health, safety and fire controls by providing adequate resources across their business activities.
- Identify and mitigate any significant risks arising that could adversely impact bank and supplier colleagues, customers or the supply chain by undertaking risk assessments of all work activities, items of equipment, processes and environments. Copies may be requested for monitoring and audit purposes.
- Provide on request evidence and information of their operational provisions to minimise risk to bank colleagues, customers or the supply chain through maintenance of all places of work, plant and equipment, storage, transportation and systems of work.
- Enable bank and supplier colleagues to take responsibility for themselves and others while carrying out their work by providing them with suitable, sufficient and ongoing instruction, training, information and supervision.
- Actively support and build a culture whereby health, safety and fire considerations are considered in all business-as-usual decisions.
- Consult and communicate on health, safety and fire matters with bank and supplier colleagues and their appointed representatives.
- All accidents and near misses arising out of the activities associated with the supplied service must be advised to the Supplier Manager including any enforcement authority engagement.

Additional Information:

All service and supply partners and contractors operating under Bank contracts are required to undergo due diligence assessments or be subjected to an agreed third-party accreditation process as appropriate to ensure that they can meet the requirements of the policy.

All business operations located outside of the UK are covered by this policy unless local host country laws and regulations set higher standards, in which case those higher standards must be followed.

Controls:

- Risk Assessments.
- Accident Reporting and Investigation.
- Mandatory Training.
- H&S Role specific (First Aiders, fire Marshals & Health Safety Coordinators).

Additional Information:

Supply Chain Partners and Contractors

Ensure that all service and supply partners and contractors operating under TSB contracts undergo due diligence assessment. TSB requirement is also that high risk contractors also hold an agreed third-party accreditation.

Name of Policy	High and Medium Events Policy

Objective:

Events in TSB are assessed using the Event Impact Matrix. Events are categorised as either Low, Medium or High. As High and Medium Events are likely to have a significant impact on TSB and / or TSB customers, the objective is to ensure the timely identification, assessment, notification and reporting of High and Medium Events.

Policy Principles:

There are three main steps to be taken when escalating a High or Medium Event.

Identification – The Event is identified (a single Event, where High/Medium thresholds for financial losses or non financial impacts have been met, and which has actually, or could potentially have, happened resulting in a direct or indirect impact.)

Assessment - the Impact Matrix should be used to assess the Event and determine whether the Event should be classified as High/Medium.

Notification – The Supplier must inform the Bank of any Medium / High Event within one working day of assessment as Medium / High.

Once an Event has been notified the Supplier will work with the Bank to ensure all appropriate corrective and remedial actions are taken to close out the Event and prevent a re-occurrence. The Supplier should provide regular updates on the progress of the actions. The Bank will record all actions on our Risk system and monitor them through to completion.

Controls:

To ensure compliance Suppliers must:

- Ensure processes are in place to enable adequate awareness and compliance with this policy.
- Ensure prompt notification of High/Medium Events to the relevant Bank contracting party. Ensure non-financial as well as financial High/Medium Events are escalated.
- Ensure full root cause analysis is undertaken for all High/Medium Events in a timely manner.
- Ensure actions are put in place and completed in a timely manner to prevent re-occurrence of High/Medium Events.
- Ensure that all information relating to High/Medium Events are readily shared with the Bank's contracting party.

Name of Policy	Information and Cyber Security Policy

Objective:

This policy is intended to establish the requirements governing the protection of data and assets against the information security risk. "The risks associated with protecting information and information systems from unauthorised access, disclosure, disruption, modification or removal." Policy is aligned to the framework and controls defined in the National Institute of Standard and Technology (NIST) Special Publication 800-53 Rev. 4.

For the purposes of this Policy, Information Security and Cyber Security are defined as follows:

- Information Security – "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." (Source: NIST SP 800-53 Rev. 4).
- Cyber Security – "The ability to protect or defend the use of cyberspace from cyber-attacks." (Source: NIST SP 800-53 Rev. 4).

The objectives of this policy can be summarised into four key requirements:

1. We must know our information assets.
2. We must know our information assets are secure.
3. We must find and fix weaknesses.
4. We must be robust when under attack.

Policy Principles

We must know our Technology and information assets and the importance to TSB:

- We maintain the technology, infrastructure, applications, and information inventory (CIO & CISO).
- We must ensure we manage and maintain an inventory of our assets in line with the guidance detailed in our technical standards (CIO).
- We must regularly conduct assessments to discover, identify and record unknown assets (CIO & CISO).
- We must ensure each asset has an appropriate owner and this ownership is recorded and maintained (All).
- We must periodically conduct assessments to calibrate and record the importance and criticality of each of our assets (e.g., those critical assets which are internet/customer facing or process payments (CIO & Records Champions).
- We must capture changes to an asset over its life cycle and in line with the guidance detailed in our technical standards (All).

We must know our assets are secure:

- We must know what 'secure' looks like in accordance with the requirements detailed in our technical security standards.
- We must regularly check that our assets are secure in line with the requirements detailed in our technical standards.
- We must understand the threats and risks which can impact our assets.
- We must create assets securely in line with the requirements in or technical standards.
- We must change assets securely in line with the requirements detailed in our technical standards.
- We must protect data by application of the required encryption for each asset.
- We must protect data as stipulated by the Payment Card Industry Data Security Standard (PCI-DSS).
- We must share assets securely in line with the requirements detailed in our technical standards.
- We must decommission assets securely in line with the requirements detailed in our technical security standards.
- We must have a security awareness training programme which ensures that users understand their duties and responsibilities in relation to Information Security. This includes an annual training to all partners and contractors.
- We (TSB) must ensure we are compliant with relevant regulatory, legal, and contractual requirements and record keeping for Information Security.

We must find and fix our weaknesses:

- We must conduct regular assessments to discover vulnerabilities and non-compliances in our assets.
- We must remediate identified vulnerabilities and non-compliances in our assets timeously.
- We must manage the risk associated with open vulnerabilities and non-compliances in line with the requirements detailed in our technical standards.

We must be robust when under attack:

- We must monitor our assets for malicious behaviour.
- We must detect instances of malicious behaviour against assets.
- We must detect propagation of malicious behaviour between assets.
- We must detect instances of discovery, collection, and exfiltration of our data.
- We must respond timeously to the detection of malicious behaviour.
- We must recover from and malicious actions against our assets within agreed timeframe.
- We must learn from the experience in order to strengthen future responses to malicious behaviour.

Controls:

Control Area / Title	Control Description
Data Security	We have process in place to: • Identify, records and assign an owner to each data asset. • Classify data in line with TSB classification and assess for retention period. • To understand threats and risks to our data assets by defining Data Leakage rules. • Secure data assets through record classification, non-production environment security controls, encryption, and access monitoring. • Test and change Data Loss Prevention (DLP) rules securely. • Share and decommission data assets share securely. • Discover and remediate vulnerabilities and non-compliances in our data assets. As well as managing risks with open vulnerabilities and non-compliances. • To detect, respond to, and recover from malicious behaviour, propagation between assets, discovery, and collection of data.

Data Security	• Learn from the experience by undertaking Post incident reviews. Data Sensitivity and Labelling – We have processes to: • Classify unstructured data using data label categories. Web filtering - We have processes to: • Prevent exposure of colleagues and systems to offensive, illegal, and dangerous web content. • Block by default access to sites which pose a security risk to TSB. • Document and maintain privileged access assigned to colleagues. • Apply a dedicated web filtering solutions to control access to websites. • Add sites to categories. • Log web access to allow production of reports. • Apply compensating controls to web sites not (yet) categorised. Secure Disposal of Information and Equipment - We have processes to: • Dispose of Information including collection, removal and destruction of information. • Dispose of equipment including secure transport. • Securely transport Highly Confidential, Confidential and Internal information. • Transport unencrypted data. Records Retention - We have processes in place to: • Classify records using defined retention categories. • Comply with legal, regulatory and operational requirements. • Handle the volume of records withing the Distribution network. • Dispose of records. • Permanently retain records. Information Classification and High-Risk Data Transfer - We have processes in place to: • Classify data. • Transfer high risk data internally and externally. • Record high risk data transfers.
Third Party Security	We have processes in place to: • Identify, record, and assign an owner and criticality for each supplier. • Ensure contracts and changes to contracts are maintained/aligned to European Banking Authority (EBA)/Financial Service Authority (FSA), legal (General Data Protection Regulations (GDPR) guidelines. • Recertify suppliers in line with treatment strategy. • Understand the significance of a supplier in a process and identify Information Security risk. • Determine security posture of a supplier is aligned to TSB information security posture. • Document any Information Security risks and approved mitigation strategies. • Retire supplier to ensure safe destruction or retention of data. • Regularly check suppliers are secure. • Identify and remediate vulnerabilities and non-compliances with suppliers. • Detect malicious behaviour.
Identify and Access Management	We have processes in place to: • Identify, record, assign an owner and assess the importance of Identity and Access assets. • Understand the threats and risks through Segregation of Duty Controls (SoD). • Secure Identity and Access assets through controls for Password and PINS, Role Based Access Controls (RBAC), Authentication requirements, Two Factor/Multi Factor Authentication, segregation of duty and Remote Session Approval. • Limit, manage and monitor privileged access. • Implement for each stage of an identity and access assets through its lifecycle with Provisioning Controls, Mover Controls, Dormancy and Leaver Controls. • Check Identity and Access assets are secure through Recertification at least annually. • Discover, remediate, and manage risk of vulnerabilities and non-compliances in identity and access assets.

Application Security	We have processes in place to: • Identify, record, assign an owner, assess the importance, and map Applications to Critical Infrastructure (CI). • Understand the threats and risks to our Applications. Development is carried out using Secure Coding Practices in secure environments. Processes and controls are in place for supplier developed Applications. • Secure Applications by maintaining a secured source code / binary code library and repository. Separation of environments and personnel. Data / information /documentation protections. • Create Applications securely including identifying and documenting security controls, using cryptographic systems and techniques, using security best coding practices, testing and approvals. • Change and share Applications securely. • Decommission securely using the Systems Development Life Cycle (SDLC) process. • Check Applications and Mobile Applications are secure including security testing. • Discover vulnerabilities and non-compliances in Applications using Vulnerability Identification, Patch management procedures and Penetration Testing. Identified vulnerabilities and non-compliances are managed and addressed prior to production implementation. • Detect malicious behaviour including Application monitoring and alerting tools.
Information Security Governance	We have processes in place to: • Identify, records, assign an owner assess the importance and capture changes of Governance assets. • Develop and disseminate an organisational-wide security plan and rolling strategy. • Secure Governance assets by understanding threats and risk and categorising Systems/Assets. • Create assets securely and regularly check they are secure. • Discover remediate and manage the risk and vulnerabilities and non-compliances in Governance assets. • Implement training and communication on the monitoring strategy. • Respond timeously to incidents. • Identify changes to policy, standards or controls following Post Incident Review.
Name of Policy	**Material Subcontractors Policy**
Objective:	
As a responsible Bank, TSB have a requirement to ensure that all goods and services are bought in a way that limits risk and provides the best value for the business while staying in full compliance with our regulatory requirements. The primary regulations that guide our approach to sourcing and supplier management are provided by the Prudential Regulation Authority: Outsourcing and Third-Party Risk Management rules and the Financial Conduct Authority requirements for Senior Management Arrangements, Systems and Controls (SYSC) – Chapter 8: Outsourcing	
Policy Principles:	
For all Supplier arrangements, we must consider sub-contracted activities that deliver services to TSB that could materially impact TSBs regulatory compliance, financial performance, and business continuity. TSB will permit the sub-contracting of elements of the service by a Supplier where the risk is deemed acceptable. Any changes to Material Sub-Contracted arrangements can only be made with the written consent of TSB. A Material Subcontractor is a supply chain partner of TSB's most critical suppliers who materially supports the delivery of contracted services to TSB	
Additional Information:	
Specific control requirements will depend upon the nature of the service or function being performed and will be confirmed to the Supplier by TSB's contracting party. Any material differences between the requirements set out above and the supplier's own controls should be raised with TSB.	

Infrastructure Security	We have processes to: • Identify, record, assign an owner, assess the importance, and capture the changes over its life cycle of Infrastructure assets. • Secure Infrastructure assets with controls for Network Management, End Point Protection and Cloud. • Regularly check Infrastructure asset are secure through external and internal vulnerability scanning and testing. • Understand threats and risks to infrastructure assets by monitoring, understanding, prioritising documenting, and tracking internal and external threats, risks and vulnerabilities. • Create assets securely by identifying and documenting Infrastructure asset controls and using cryptographic systems and techniques. • Change and share Infrastructure assets securely. • Decommission Infrastructure assets securely considering the System Development Life Cycle (SDLC) procedures. • Discover vulnerabilities and non-compliances through vulnerability identification and patch management procedures, vulnerability scans and end point scanning and monitoring. • Remediate and manage the risk associated with vulnerabilities and non-compliances identified on infrastructure assets. • Monitor for and detect malicious behaviour.
Key Management	We have processes to: • Identify, record, define roles and responsibilities, assign an owner, asses the importance and know the threats for each Encryption asset. • Secure Encryption assets including managing access controls, generating, and deleting key and credentials securely, training and awareness plans, defining and implementing Public Key Infrastructure (PKI), encrypting data throughout lifecycle, implementing and testing recovery plan, collecting sufficient logs and performing maintenance securely. • Detect and respond to threats. • Understand impact of key and credential compromise, implement robust recovery processes, contain, and mitigate compromises, continuously improve response to attacks.
Security Operations	We have processes in place to: • Manage, monitor, and report incidents. • Develop and implement an incident response plan. • Conduct incident training and testing and provide incident response assistance. • Define information flows. • Define, record, analyse and report auditable events. • Protect audit information. • Protect against malicious code and spam. • Monitor systems and information. • Define and execute software, firmware, and information integrity. • Monitor systems and information. • Monitor and control remote access methods. • Receive, generate, disseminate, and implement information system security alerts, advisories and directives. • Implement a threat awareness program.

Additional Information:

Specific control requirements will depend upon the nature of the service or function being performed and will be confirmed to the Supplier by TSB's contracting party.

Any material differences between the requirements set out above and the supplier's own controls should be raised with TSB.

Based on the nature and materiality of the service provided by 3rd parties, they may be subject to requirements to support internal and external audits of TSB and other assurance related activity as required by regulations that TSB is subject to.

Name of Policy	Operational Resilience Policy

Objective:

The objective of the Policy is to set out the requirements for implementation of robust business continuity management practises for the Bank.

- We care about ensuring the continuity of business operations and protection of Partners,
- contractors, agency staff, customers, and the Bank's reputation.
- We constantly strive to do the right thing, implementing appropriate operational resilience measures and recovery planning in alignment with the Financial Conduct Authority (FCA) & Prudential Regulation Authority (PRA) expectations within SYSC 4 to establish, implement & maintain adequate Business Continuity Policy. In implementing the new UK operational resilience regulation, we are identifying where we are dependent on suppliers to deliver our important business services and will look to assess the resilience of these dependencies to give confidence that we can stay within our impact tolerances for severe but plausible scenarios.

Policy Principles:

- Reduce the likelihood and impact of interruptions whilst supporting the Bank's values, strategy, and business goals.
- Clearly explain the responsibilities of a) all Partners, contractors and agency staff and b) those directly involved in or accountable for Business Continuity Management
- Meet regulatory requirements.
- Ensure an effective response to incidents caused by any threat to the Bank through the development of effective incident management procedures and plans.
- Minimise the impact of incidents through effective operational resilience measures, proportional to risk in the business.
- Ensure an effective recovery from incidents caused by any threat to the Bank through the development of effective continuity plans.
- Provide the overarching framework and governance.
- Ensure Business Units have recovery capability, processes and agreed timescales in place for the recovery of the Bank's critical operational activities.

Controls:

Supplier Requirements

Suppliers must ensure and confirm that business continuity provisions are in place which are in line with the requirements of the TSB policy and can recover services to TSB to an acceptable level ahead of the Maximum Tolerable Outage (MTO) value set by TSB, including:

- **Incident Response Structure** – A documented process to identify, escalate and manage the impact of incidents.
- Criticality – Identify, assess, and classify activities (and their dependencies) relative to the impact their interruption would have on TSB.
- Survival Critical – Could put the survival of the Bank at risk.
- Business Critical – Could have a material or significant impact on third party supplier and the Bank.
- Non-Critical – Would not have a material or significant impact on the third-party supplier and the Bank within the first 30 days following the identification of the incident.
- **Continuity Strategy** – development of strategies for:
- Denial of people (Including Pandemic)
- Denial of premises
- Loss of technology (inc. Telephony)
- Loss of data / information
- Supplier failure through own supply chain (4th Party to TSB)
- **Incident Response and Business Continuity Plans** – provide a documented framework for managing an incident and any subsequent recovery based on agreed objectives, timescales, and activities.
- **Testing and exercising** – provide assurance that that the Incident Response and Business Continuity Strategy and supporting plans remain fit for purpose

Additional Information:

Specific control requirements will depend upon the nature of the service or function being performed and will be confirmed to the Supplier by TSB's contracting party.

Any material differences between the requirements set out above and the supplier's own controls should be raised with TSB.

Name of Policy	Payments Policy

Objective:

Payment Services Regulations are gaining ever-widening scrutiny from Governments, Regulators and Consumers over management of payment transactions. With new innovation in the payments industry there has been an evolution in how customers can make payments and TSB must ensure that customers continue to make compliant payments through differing channels.

The Payments Policy primarily covers any electronic and cheque payments processed by TSB and is underpinned by the 2017 Payment Service Regulations.

TSB has a prudential responsibility to ensure that it operates in a compliant and responsible manner for its customers, stakeholders and partners.

If TSB failed to comply with this Policy this would be detrimental to the customer causing a negative customer experience and would go against TSB values.

Policy Principles:

The Standards that the TSB Payments Policy incorporates are:

Payment Standards - Gives detail of what business units and suppliers should be doing to be compliant with policy. The standards also outline the payment service regulations TSB are required to comply with.

Single European Payment Area (SEPA) Standards -The SEPA End Date Regulation aims to standardise Euro Payments and to ensure that it is as easy for customers to make Payments to other countries within the European Economic Area (EEA) as they can be made domestically, with the same experience for customers and these are the standards that need to be met in relation to this.

Clearing Standards – The Clearing standards detail the measures that need to be taken by TSB to process cheque payments in compliance with the Image Clearing System rules.

Controls:

Suppliers must ensure the following:

1. Governance and controls are in place to support any part of the end-to-end payments process.
2. When acting on a customer's instructions there must be certainty that instruction has been given by a genuine customer, it is not fraudulent and falls within the permission granted by the account/product authority.
3. All required information related to a payment is provided and remains throughout the payment chain to allow sufficient payments screening in-line with the TSB Sanctions and Related Prohibitions Policy.
4. Compliant operational processing.
5. (All Payment Services Regulations are adhered too.

Additional Information:

Specific control requirements will depend upon the nature of the service or function being performed and will be confirmed to the Supplier by TSB's contracting party.

Any material differences between the requirements set out above and the supplier's own controls should be raised with TSB.

Name of Policy	Physical & People Security Policy

Objective:

We care about protecting our Customers and Colleagues safety and maintaining our customer's confidence and we show this through management of Physical & People security risks. We are passionate about protecting the Bank's Commercial interests and reputation ensuring we comply with legal requirements and meet regulatory expectations. We do this by ensuring:

- Any person employed by, or contracted to work for on behalf of the Bank and any person visiting Bank premises are protected against actual or threatened harm caused by a Physical Security Incident.
- Any property belonging to the Bank or which the Bank has responsibility for is protected against theft or damage.
- Any premises from which the Bank operates is protected against unauthorised access, intrusion, or damage.
- All Colleagues and third-party suppliers understand their responsibilities for ensuring appropriate risk management of Physical & People Security across the Bank.

Policy Principles

Accountability – Where restricted access areas exist, each relevant Business Unit will appoint a Business Unit Accountable Access Co-Ordinator (BUAC) to manage their physical access rights for their Business Area.

- Risk & Threat Assessment – Each Business Unit will complete a comprehensive risk & threat assessment covering all of the physical & people security threats facing their business.
- Access Control – All colleagues should be aware of their responsibilities and procedures surrounding physical access control.
- Incident Management – All of our Business Units will ensure that all suspected or actual physical and people impacting incidents are reported in line with the Bank's Incident Management Guide.
- Property – Our Property department will take responsibility for managing the security arrangements at properties where they provide managed facilities services.
- Sourcing & Supplier Management – Our Sourcing department, along with the Business Units, will ensure that all contracts with 3rd party suppliers contain and adhere to the security requirements detailed in our Security Schedule.

Controls

- Core Learning for TSB colleagues to complete.
- Access controls for all restricted areas.
- Personal security reviews
- Documented security measures for the TSB branch network.
- Contractual clauses for suppliers that adhere to TSB's Security Schedule.

Additional Information

Name of Policy	Pre-Employment Vetting Policy

Objective:

As a major employer, the Bank is committed to adopting the highest standards in this process, employing individuals who demonstrate the appropriate skills, experience and integrity. Additionally, the Bank has a responsibility to its customers and shareholders to deter, detect and disrupt any attempt at financial crime. The screening of potential recruits to the Bank is an importance defence against fraud.

Pre-employment screening is the process of ensuring that sufficient information about each potential recruit is acquired in order to demonstrate that they meet the standards required for employment in their proposed role within the Bank.

Policy Principles:

The policy defines the fundamental requirements for the pre-employment screening of potential recruits, whether permanent or temporary. These requirements must be satisfactorily completed for each potential recruit prior to starting their role with us.

Role Categories

This Bank adopts a risk-based approach to role classification and defines four categories of role. These cover all roles in the Bank. The role category determines the pre-employment vetting standards that must be applied before the potential employee's start date within the Bank.

All roles across TSB are assigned a Role Category, which determines the level of screening required. For example, a higher level of screening is required for those candidates who are being recruited into roles which are regulated by the FCA.

Non-Permanent Standard applies to all individuals not directly employed by TSB unless the role falls into a SMCR categorisation.

Standard applies to all individual who are recruited new into TSB who do not fall into any of the below categories.

TSB Volume applies to all individuals who are recruited new into TSB into one of our customer facing roles where the first few weeks are spent in a fully supervised training environment.

Certification Regime/ Material Risk Taker applies to all individuals recruited into a role in scope of the Certification Regime, predominately when a CeMAP qualification is required for the role or their line manager and those roles which TSB has identified as Material Risk Takers.

Senior Managers Regime applies to all individuals recruited into a role at board level or Non-Executive Director level

Vetting Requirements TSB conducts screening checks across a number of fields including: Right to Work, Criminal Record Checks, Sanctions and Politically Exposed Persons, CiFAS, Credit Checks, Media Searches, Employment/Education References and, where appropriate Directorships and Professional Qualifications.

Controls:

Suppliers must ensure they:

- Adhere to all relevant legal and regulatory requirements.
- Do not engage in any illegal, improper or questionable conduct that breaches the Bank Policy,
- Have in place an effective mechanism to implement and assess compliance with the Policy, including retaining evidence of screening.
- Clearly explain to those individuals acting on behalf of the Bank their personal responsibilities in relation to pre-employment screening.
- Encourage high moral and ethical standards in all business activities.

Where a supplier is unable to meet the screening standards they must work with the policy owner to either remove the obstacle or agree a suitable alternative. Suppliers are also expected to regularly demonstrate their ability to meet the pre-employment screening standards and submit to audits at agreed intervals.

Additional Information

Specific control requirements will depend upon the nature of the service or function being performed and will be confirmed to the Supplier by TSB's contracting party.

Any material differences between the requirements set out above and the supplier's own controls should be raised with TSB.

Name of Policy	Technology Resilience Policy

Objective:

The purpose of this Policy is to support TSB to deliver IT services which meets customers' expectations, supports TSB's business strategies and complies with all regulations and applicable laws, and manage Technology Risk within TSB's Risk Appetite.

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

1. PRA Rulebook: Capital Requirement Regulation / Solvency II Firms
2. FCA Handbook: Systems and Controls
3. Senior Management and Certification Regime (SM&CR)
4. Bank of England
5. European Banking Authority guidelines on ICT

Where instances of non-compliance are identified, risks will be defined and either risk accepted or mitigating actions managed to completion.

We define Technology Risk as "the failure to provide or maintain technology systems, architecture or disaster recovery for both TSB owned or Cloud based services leading to unavailability of services to customers, and longer recovery times, ability to respond to any disruption, demand or threat and continue Critical Business Services within acceptable levels".

Policy Principles

- Ensure that adequate capacity is available at all times to meet the agreed needs of the Business in a cost-effective manner.
- Document and implement a service readiness approach, which is reviewed annually.
- Manage the controlled deployment of software for in-scope applications.
- Ensure that technology change management is appropriately recorded, assessed and implemented into TSB's production environment in a controlled manner.
- Manage and respond to any events that occur and act on any alerts that are triggered by our critical applications.
- Respond and restore service after an incident has occurred.

Controls

- Track all configuration items in an IT system.
- Maintain software and technology infrastructure.
- Ensure that problems are identified, and a root cause analysis is undertaken to ensure the minimalization of recurring incidents.
- Keep a backup of all files and store them securely in case recovery actions are required.Ensure all documentation is in place to help us to manage and respond to any incidents in a correct manner.

Additional Information

Name of Policy	Vulnerable Customers Policy

Objective:

The Vulnerable Customer Policy is designed to ensure that the fair treatment of vulnerable customers is always considered and that vulnerable customers experience an outcome as good as those of other consumers.

Policy Principles

The Vulnerable Customer policy aligns to FCA Guidance on the fair treatment of vulnerable consumers and covers the 6 key focus areas:

- Understanding the needs of vulnerable customers.
- Customer service.
- Product and service design.
- Communication.
- Skills & capability of staff.
- Monitoring and evaluation.

Controls

- A Vulnerable Customer Policy.

Additional Information

Specific control requirements will depend upon the nature of the service or function being performed and will be confirmed to the Supplier by TSB's contracting party.

Any material differences between the requirements set out above and the supplier's own controls should be raised with TSB.

Name of Policy	Whistleblowing Policy

Objective:

We care about our customers and our colleagues and strive to do the right thing. We do this by encouraging colleagues to report concerns of wrongdoing or inappropriate behaviour which could impact customers, colleagues, or TSB; knowing that their concerns will be investigated promptly and effectively without fear of reprisals for them.

We encourage all colleagues to have transparent and trusting relationships with their line managers as a first point of contact. If they are not comfortable reporting a concern to their line manager or a suitable alternative, the Whistleblowing process provides the opportunity for them to do so confidentially and, if they wish, anonymously.

Controls:

- TSB must appoint a non-executive director as "Whistle-blowers' Champion", with the responsibility for ensuring and overseeing the integrity, independence and effectiveness of the firm's policies and procedures on whistleblowing.
- We must make it easy for concerns of wrongdoing to be raised in the strictest confidence.
- We must ensure that colleagues raising concerns do not suffer any detrimental impact from raising those concerns or suffer any form of victimisation.
- All Whistleblowing concerns are to be thoroughly investigated.

Additional Information:

Specific control requirements will depend upon the nature of the service or function being performed and will be confirmed to the Supplier by TSB's contracting party.

Any material differences between the requirements set out above and the supplier's own controls should be raised with TSB.