Yorkshire Building Society

Procurement & Third Party Risk Policy Overview

Updated August 2023

Contents

1. Purpose

The Purpose of the Policy

The Procurement, & Third-Party Risk Policy is intended to set out at a high level the Society's attitude towards third party risk and the steps which must be taken in order to identify, assess and manage this risk.

The Society's ability to provide 'real help with real lives' is dependent upon its ability to provide uninterrupted value adding services to its customers. The provision of such services is in part dependent upon third party suppliers.

Failure to effectively manage the risks associated with the selection, management and oversight of third-party suppliers, may lead to deterioration / failure in service, potential regulatory breach, unplanned costs and reputational damage.

Applicable Regulations and Legislation

Following the Policy will support compliance with the Society's statutory and regulatory obligations including:

- Bribery Act 2011
- CEBS(Committee of European Banking Supervisor)
- EBA (European Banking Authority) guidelines on Outsourcing arrangements EBA GL/2019/02
- FG 16/5 FCA (Financial Conduct Authority) guidance for firms outsourcing to the 'Cloud' and other 3rd party services
- Modern Slavery Act
- PERG 4.15 Mortgage activities carried out by 'packagers'
- PRA (Prudential Regulation Authority) outsourcing rule book
- PRA Prescribed Responsibility u-a
- SMF24 Chief Operations Function
- SYSC (Systems and Controls Sourcebook) 8.1 General outsourcing requirements
- SYSC 13.9 Outsourcing
- SUP 2.3 Information gathering by the FCA on its own initiative: cooperation by firms
- SUP 15.3.8 General FCA notification requirements
- UK GDPR & DPA 2018

Requirements of the Policy

All colleagues whose role involves working with third party suppliers need to understand and follow this policy and the associated policy guide.

2. Scope

This policy applies to all YBS colleagues and contingent workers where their role involves working with third party suppliers.

The Policy excludes;

- All Lending/Distribution third parties who are already on or apply to join the Accord panel. These third parties are managed in accordance with the Accord Mortgages Governance and Oversight Framework.

- Agency Agreements; where the Society appoints an agent on a non-exclusive basis as its agent to continue to carry out the business at their premises.

This policy relates to the management of risk to the Society in relation to the selection, management and oversight of third-party suppliers.

3. Definitions

Third Party

A third party is a supplier who provides services, goods, leases, or licenses under a contract.

Procurement

The process used by the Society in order to define a requirement for goods or services, identify and assess potential third parties, select a preferred supplier and complete contractual arrangements.

Third Party Risk Management

The process used by the Society in order to ensure that the risks associated with the use of a third party are identified and assessed and such risks are appropriately managed. The Outsourcing & Third-Party Risk process is integrated within both procurement and supplier relationship management activities and is aligned to the Societies Enterprise Risk Management Framework (ERMF).

Risk & Control Self-Assessment (RCSA)

A periodic review performed by each business area in order to determine whether risks are being effectively managed, associated controls are fit for purpose and operating as expected.

Supplier Relationship Management

The process used by the Society in order to ensure that goods and services provided by a third party supplier are received in accordance with the contract and any associated service level agreements, the anticipated benefits associated with the contract are achieved and any contract change, renewal or termination are effectively managed.

Supply Chain Management Team

The team responsible for ensuring that the Society has an appropriate policy, procedures, and systems in place in order to:

- Understand and continue to meet its statutory and regulatory responsibilities in relation to procurement of goods and services and the subsequent management of third-party relationships;
- Obtain value for money and receive goods and services that are of appropriate quality;
- Ensure that the risks associated with the use of third parties are identified and are managed effectively in order to assure that services remain operationally resilient.

Colleagues - YBS employees (permanent and temporary).

Contingent workers - Individuals who work for or with YBS through either their own Limited Company, a 3rd party company or employed by a YBS agency. This category is often referred to as either a contractor or consultant.

Must - The use of 'must' in this policy conveys a mandatory requirement to be undertaken.

Supplier Concentration Risk

Supplier concentration risk is defined as the likelihood of loss or impact arising when the Society relies too heavily on too few suppliers to perform critical or important services that could impact the successful achievement of the Society's objectives.

The following three types of supplier concentration risk apply. Identification of the following risks when on-boarding a third party is mandatory with a clear plan to mitigate or manage those risks must be evidenced:

- **Service Provider Concentration** – Occurs when the Society has a supplier(s) who provide more than one service to the Society or the same service across multiple business lines, as a result of being over-exposed and reliant upon just a few counterparties to deliver critical or important services.

For example, service provider concentration can occur when a single service provider is providing i) multiple services along a single important business service and/or ii) services across multiple important business services.

- **Geographical Concentration** – Occurs as a result of the Society outsourcing services to a cluster of suppliers that are located in a single geographical area.

For example, outsourcing to multiple suppliers co-located in a single geographical region in India that could be impacted by infrastructure risks (i.e. energy supply cuts). Or where multiple services are delivered from one central office of operation.

- **Supplier Customer Concentration** – Occurs when an outsourcer is dependent on the Society for its ongoing viability. Customer concentration occurs when the Society represents more than 20% of a supplier's overall revenues.

Service Provider and Geographical Concentration measures are in place and tracked via the Supplier Concentration Log and reviewed at the Operational Risk & Resilience Forum.

Outsourcing

An arrangement of any form between an institution, a payment institution or an electronic money institution and a service provider by which that service provider performs a process, a service or an activity, or parts thereof that would otherwise be undertaken by the institution, the payment institution, or the electronic money institution itself.

As a general principal, the following examples do not meet the definition of outsourcing:

- A function that is legally required to be performed by a service provider;
- Financial market information services, such as Bloomberg or Moody's;
- Global payment network infrastructures, such as Visa or MasterCard;
- Correspondent banking services; and
- Acquisition of services, e.g. architect, legal representation, goods, utilities.

Critical or Important

An arrangement should be considered 'Critical or Important' where a failure to that service (provided by the supplier to the Society) could cause a material impact upon the Societies ability to service its customers and/or comply with existing laws and regulations.

Examples of a material impact are as follows:

- Where a supplier's service failure could interrupt the Societies payment system; resulting in customer inbound or outbound transactions being delayed or incorrectly processed.
- Where a significant amount of YBS customer data held by a supplier is compromised, for example; through a data loss or cyber-attack. Sensitive customer personal data, as defined under GDPR, should always be considered as 'Critical or Important.'

Therefore, examples of an outsourcing arrangement considered 'Critical or Important' are as follows:

- Outsourcing of key internal controls functions, such as 2nd LoD monitoring & oversight and 3rd LoD internal audit assurance.
- Outsourcing of significant parts of the Societies operational infrastructure, e.g. Target providing mortgage servicing to Accord mortgages and N&P 'Buy-to-Let' mortgages.

According to the FCA rulebook (SYSC 8.1.5), the provision to the firm of advisory services which do not form part of the relevant services and activities of the firm, including provision of legal advice to the firm, the training of personnel of the firm, billing services and the security of the firm's premises and personnel should not be considered Critical or Important. Moreover, the purchase of standardised services, including market information services and the provision of price feeds should also not be considered Critical or Important.

Material Outsourcing

According to the FCA handbook (SYSC), material outsourcing is defined as outsourcing services of such importance that weakness, or failure, of the services would cast serious doubt upon the firm's continuing satisfaction of the threshold conditions or compliance with the principles.

Intra-Group Outsourcing

Intra-group outsourcing is an arrangement in which one company within a group of companies provides services for another company within the same group that could also be or usually have been provided in-house. Services provided to Accord Mortgages Limited by Yorkshire Building Society are considered the only material intra-group outsourcing agreement within the YBS group. Intra-group outsourcing is subject to the same regulatory requirements as external outsourcing relationships.

According to the FCA rulebook (SYSC 13.9.3), a firm should not assume that because a service provider is either a regulated firm or an intra-group entity an outsourcing arrangement with that provider will, in itself, necessarily imply a reduction in operational risk.

Cloud Computing

In common terms, cloud computing is defined as a model that enables on-demand network access to a shared pool of configurable computing resources, that is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services, that can be rapidly provisioned and released with minimal management effort or service provider interaction).

As set out within the Cloud Computing Strategy (March 2019), Cloud hosting options include;

- **Public;** a hosting approach where computing resource is shared by multiple organisations and made available over the internet,
- **Private;** a hosting approach optimised, segregated, and served for a single organisation and
- **Hybrid;** a hosting approach that consists of a combination of Public and Private Cloud.

4. Policy Statements

Adherence to the following policy statements should ensure that the risks associated with third party suppliers are managed consistently and effectively across the Society and through all stages of the supply chain lifecycle.

Strategy & Mandate

- YBS' Board expects the Society to achieve advanced third-party risk management enabling simply brilliant mortgages and savings whilst ensuring value for money, operational resilience and fair customer outcomes.
- YBS like many financial institutions is exposed to third party risk as part of its day-to-day operations. YBS' risk appetite towards third party risk helps to achieve its commercial objectives, whilst mitigating third party risk through the effective implementation of key controls.

- YBS' attitude to third party risk has been set out within a set of documents, including but not limited to the Third-Party Risk Appetite, Policy, Policy Guide and Minimum Supplier Standards.

Framework

- The Supply Chain Management Team is responsible for developing and maintaining the Society approach to third party supplier risk management, including the Procurement, Third-Party Risk policy guide and associated risk assessment methodologies.
- The Procurement, Third-Party Risk policy guide and associated risk assessment methodologies must be periodically reviewed and approved by the Operational Risk & Resilience Forum.
- The Society approach to third party risk management must at all times remain aligned and respond where appropriate to changes in the Enterprise Risk Management Framework (ERMF). For the purpose of clarity, the ERMF will always take precedent.
- The Society's Chief Officer Direct Reports (CODRs), which comprises the Directors or colleagues with delegated authority, must ensure that third party risk management is effectively performed within their areas of responsibility.

Risk Appetite

- Risk appetite for third party risk will be encompassed within the Society's operational risk appetite, which must be reviewed and endorsed on an annual basis by Executive Risk Committee (ERC) prior to being submitted to Board for approval. The risk appetite statement(s) articulates the nature and level of third-party risk that the Society is willing to take in pursuit of its strategic objectives.

Risk Governance & Committees

- The Society must have a governance structure for third party risk management, with defined responsibilities and clear lines of escalation. Currently this consists of the Operational Risk & Resilience Forum with escalation as required through the Customer Services Division Risk Committee (CSDRC) and up to Board.
- All suppliers must follow YBS minimum standards. Minimum standards expected of YBS' suppliers have been defined and can be accessed via YBS' external website (https://www.ybs.co.uk/your-society/inside-your-society/corporate-governance/policies/index.html).
- YBS must record and maintain a central register of all outsourcing arrangements (including those using a Cloud computing service), regardless of whether they have been assessed as Critical or Important. The PRA has the right to ask for a copy of this register at any time. Where the PRA requests this information, this will be done via the YBS Regulatory Strategy & Change team.

Procurement

- Sourcing requirements over £50k (inc. of VAT) must be referred to Procurement to conduct a competitive tender process
- Any proposed consultancy spend must be referred to the Chief Executive for approval. Use of any Tier 1 consultancy providers must be pre-approved by the Senior Supply Chain Manager.
- All third party spend unless agreed as an exception with the Supply chain Management Team must be confirmed to the third party supplier by a Purchase Order.
- Business areas must engage with the Supply Chain Management Team before engaging a new Supplier and must have the approval of their Director.
- Business areas must engage with the Supply Chain Management Team before commissioning additional or new goods or services worth over £50k from an existing Supplier.
- The end to end process for the goods or services must be fully defined and documented prior to contract signature.
- For High and Medium Risk suppliers, concentration risks associated with the potential supplier must be identified, assessed and mitigated, as appropriate. Supply Chain Management must ensure that these

identified concentration risks are consolidated into a supplier concentration log and tracked by the Operational Risk & Resilience Forum.

Due Diligence & Risk Assessment

- The Supply Chain Management Team must ensure there is a due diligence process which includes activities to identify, assess, monitor, manage and report third party risk exposures.
- The Supply Chain Management Team must ensure that the third-party risk and control library is maintained, and key controls are effectively communicated to all relevant colleagues.
- Due diligence must be completed before a contract or Contract Change Note (CCN) is signed and the Supplier is allowed to start work. This must assess the strategic alignment and capabilities of the third-party supplier and the risks to which it might expose the Society.
- The Information Security Risk Team must follow their IRM Supplier Assurance Procedure, including supplier create review, security tiering assessment, supplier assurance report certification and periodic re-certification.
- Segmentation must be completed to determine the required nature and frequency of ongoing monitoring and engagement with the supplier, commensurate with the level of risk to the Society.
- All colleagues are responsible for ensuring that third party risk exposures are identified, and risks are escalated in accordance with the ERMF and local business function procedures.
- For High and Medium Risk suppliers, the Relationship Manager must update due diligence at least annually. For Low Risk suppliers, this must be done at contract renewal. Due diligence updates must also be done if the service being delivered changes or if another significant event occurs.
- The Supply Chain Management Team must ensure that for high and medium risk suppliers, supplier concentration risks are periodically reviewed and recorded within the relevant Risk Register (RIIC Log) and a consolidated supplier concentration log is tracked at Operational Risk & Resilience Forum.

Contracts

- Where YBS contract terms have not been included in a Request for Proposals (RFP), any proposed contract terms provided by a Supplier must be sent to Group Legal, allowing sufficient time for review prior to the Supplier being engaged.
- YBS contracts with the supplier must afford YBS, its auditors, its regulators with access to data related to outsourced activities, as well as to the business premises of the service provider. Moreover, contracts must allow regulators to be able to exercise those rights of access.
- Once the contract wording has been reviewed by Group Legal, the contract must be approved in accordance with the Society Contract Signing Mandate.
- All contracts and Contract Change Notes (CCNs) must meet the Society's relevant minimum performance standards and requirements in relation to Business Continuity, Information Security, Data Privacy, Vulnerable Customers and Health & Safety. Minimum standards expected of YBS' suppliers have been defined and can be accessed via YBS' external website.
- If a third party supplier is unable or unwilling to meet the Society's relevant minimum performance standards and requirements, where it is determined to be in the wider interests of the Society and its customers to proceed, the non-compliance process, as set out within the Procurement, third party risk policy guide, must be followed.
- Contracts and CCNs must be signed by both parties prior to the purchase of the goods or commencement of the service. A copy of the signed contract/CCN must be sent to both the Supply Chain Management Team and Group Legal.
- The Supply Chain Management Team must ensure that a CODR is identified as accountable for each third-party supplier. Where different, the name of the person responsible for managing the relationship with a third-party supplier must also be recorded.

- Details of all new contracts must be recorded within a contract database and subject to periodic review to ensure the information remains up to date.

Supplier Relationship Management

- CODRs must ensure that within their areas of responsibility the performance of any third-party supplier(s) is monitored in line with the contract and that the supplier(s) remains compliant with contractual requirements and that service expectations and quality standards are maintained.
- CODRs who have payments to Suppliers included in their budgets must track spend against the contract to prevent any overspend and ensure anomalies are investigated and managed.
- Contracts contain legally enforceable obligations for the Society as well as for third party suppliers. The person responsible for managing the relationship with a third-party supplier must know what these are and must ensure that they are complied with.
- CODRs must ensure that spend and anticipated benefits are realised and tracked to identify whether the contract generates a net benefit to the Society.

Exit Plan

- The person responsible for managing the relationship with a third-party supplier must ensure that an exit strategy and plan are documented for each supplier (reflecting the agreed exit conditions).
- The plan must be reviewed and updated on an annual basis, or in the event of a significant change, to ensure that it remains appropriate.

Risk Control

- CODRs must ensure that key controls are effectively applied in order to manage third party risk exposures across the Society's activities, in accordance with risk appetite.
- CODRs must ensure that third party risk exposures are monitored across their area of responsibility, including review through Risk & Control Self- Assessment (RCSA) of the effective operation of controls which mitigate these risks.
- The Supply Chain Management Team must undertake assurance over the operating effectiveness of key third party controls across the Society. N.B. In order to operate in a risk-based and commercial manner, the extent of assurance undertaken over controls as part of this assessment should typically be commensurate to:
    - The Society's agreed risk appetite;
    - The materiality of the (Gross) risk;
    - The cost of undertaking assurance over the control; and
    - The practicality of performing the assurance.

Risk Events

- CODRs must ensure that when risk events have arisen as a result of a failure on the part of a third-party supplier, they are escalated and reported, in line with applicable YBS and local processes.
- Steps must be taken to understand the cause of third party originated risk events, the actions required to prevent reoccurrence and the cost/benefit of these actions.

Risk Reporting

- Risk reporting must be undertaken to ensure that visibility of the Society's third-party risk exposures is maintained.
- Third party risk reporting must be produced in support of the operation of the Operational Risk & Resilience Forum and Customer Services Division Risk Committee (CSDRC).

Material Outsource and Material Third Parties

- All requirements set out within the Policy and Policy Guide (Framework) also apply to arrangements that have been assessed as 'Critical or Important' (Material Third Party) or 'Critical or Important and Outsourcing' (Material Outsource).
- Arrangements that have been evaluated as Material Third Parties (Critical or Important) must be subject to a risk assessment, endorsed by the accountable Chief Officer approved by the Executive Risk Committee and notification made to the PRA, prior to the contract being signed.
- As part of YBS' supplier segmentation model, suppliers supporting Critical or Important services must be rated at least Medium Risk and accordingly follow governance requirements, as specified within the Procurement, Third-Party Risk policy guide.
- Following approval of the material outsourcing arrangement by the Board, but prior to signing contracts, the accountable Chief Officer must ensure that the Prudential Regulation Authority (PRA) is provided with details of the proposed Outsourcing arrangement and sufficient time to review the proposal.
- As part of the periodic risk assessment undertaken for all suppliers or through ongoing supplier relationship management where a material change to arrangements is noted, these arrangements should be re-evaluated to check whether they are now Critical or Important Outsourcing. If circumstances have changed and arrangements are now considered Critical or Important, the aforementioned requirements must be followed.
- As part of the risk assessment undertaken, the 'principle of proportionality' should be used. This principle aims to ensure that governance arrangements are consistent with the nature, scale, individual risk profile, business model and complexity of activities being undertaken by the outsourcing firm.

Cloud Computing

- Where a supplier arrangement uses Cloud Computing services, the relationship manager must ensure the Cloud Outsourcing Register is completed and sent to the PRA,
- Arrangements that have been identified as using Cloud Computing services must be subject to a risk assessment. Where the arrangement is also assessed as Critical or Important, the supplier arrangement must be approved by the Customer Services Division Risk Committee.
- Should an information security supplier assurance review be required, the supplier assurance questionnaire should include questions to enable the Information Security Risk team to better understand the specific Cloud computing arrangement and the associated risk profile.

5. Implementation and Monitoring

Implementation

To assist the Chief Operating Officer (SMF24) and Director of Shared Services & Resilience (Third Party Risk Category Owner) in implementing this policy, the following committees and forums have a number of responsibilities:

- **Group Risk Committee (GRC) -** A Board Committee with delegated authority to oversee Operational Risk, Compliance & Conduct Risk; Prudential Risk; and Business Risk – Strategy, Appetite and Oversight. The committee reviews the Society's operational risk capability (including third party risk) at least annually. The Board approves the policy annually.

- **Executive Risk Committee (ERC) -** the ERC is a sub-committee of the GRC. It has delegated authority from the GRC to ensure the Society's balance between seeking opportunity and managing risk is appropriate. The ERC monitors and reviews the risk exposures of the Society in accordance with the Enterprise Risk Management Framework, Risk Appetite, Group Strategy and the Corporate Plan, and

ensures clear reporting of risk exposures to the GRC and the Board. Outsourcing arrangements assessed as Critical or Important must be reviewed and approved by ERC.

- **Customer Services Division Risk Committee (CSDRC) -** is a 1st LoD committee which monitors the risk profile of the Customer Services Division to ensure that the potential impact of risks which are owned by the Division are managed within the Board's risk appetite.
- **Operational Risk & Resilience Forum -** reports to the CSDRC and is responsible for reviewing third party risks, reporting on risk events across the Society, addressing emerging trends, ensuring the Society remains compliant with this policy and policy guide, tracking corrective actions and reviewing relevant MI.

- The policy owner will ensure that the policy is implemented in practice and will inform owners of other related policies where new or significant changes are made to this policy.

- This policy and future changes will be communicated via internal communication channels including the Society's internal intranet platform (accessible by all colleagues) and email communication to key stakeholders.

- The owners of related policies (e.g. information security policy) must undertake the required review and any subsequent amendments to their own policies to ensure they are aligned with this policy.

- The implementation of this policy will be supported through ongoing training, including masterclasses provided to OpCo, Risk Policy owners, High and Medium Risk relationship managers and other colleagues, as required.

Monitoring

The Society operates a Three Lines of Defence (LoD) approach towards risk management. Each LoD has different responsibilities for managing the risk and therefore carries different actions.

The first LoD is directly responsible for the day to day management and control of risk throughout the business, generally within business functions. They monitor the implementation of this policy through:

- Each Chief Officer Direct Report (CODR) being responsible for ensuring that their function complies with this Policy and specifically that third party risks are identified, assessed and managed within the prevailing risk appetite and that key controls are operated as defined in the risk and control library.

- The Supply Chain Management Team from time to time reviewing performance against key controls as defined in the risk and control library, highlighting non-performance to the Operational Risk & Resilience Forum and escalating to the Customer Services Division Risk Committee (CSDRC) where appropriate.

The second line is accountable for competent risk management across the society and overseeing the effectiveness and integrity of the Enterprise Risk Management Framework. They monitor the implementation of this policy through various activities defined in the annual Compliance Monitoring Plan.

The final LoD is providing independent assurance across the first and second LoD through our internal Audit function. They monitor the implementation of this policy through various activities defined in the annual Audit Plan.

6. Approval

The policy must be reviewed at least annually but may be updated more frequently in the event of significant changes to, legal / regulatory requirements, related activities and processes, or to the external environment within which the Society operates.

Subject to endorsement from the Policy Sponsor, the Policy will be reviewed annually and approved by the Board.