payments and crypto network

Compliance Arrangements

A series of guides addressing operational compliance issues for UK authorised Electronic Money Institutions ("EMI") and Payment Institutions ("PI").

Guidance is provided for firms and is not intended as legal advice.

Guide 4: Outsourcing arrangements

Background

UK authorised EMI and PI businesses must adhere to the regulatory requirements defined in the Electronic Money Regulations 2011 ("EMR") and the Payment Service Regulations 2017 ("PSR") as well as and associated guidance from the UK's Financial Conduct Authority ("FCA").

In addition, following the UK's exit from the EU, the FCA continue to expect the firms that they regulate to comply with, to the extent that they remain relevant, guidelines published by the European Banking Authority ("EBA Guidelines"). One such set of EBA Guidelines are those relating to outsourcing arrangements (reference: EBA/GL/2019/02).

Firms may outsource functions that are required to deliver their regulated services, either in whole or in part, to service providers (who may be within or outside the firms' group of companies). The EBA Guidelines on outsourcing require EMI / PI businesses to maintain an 'Outsourcing Policy'; the EBA Guidelines are comprehensive and their guidance is also addressed here – ***Compliance arrangements Guide 5: Outsourcing Policy***.

This guide provides an overview of the outsourcing arrangements that should be maintained by an EMI / PI, specifically the control environment operated within these firms.

Responsibility

Responsibility for the maintenance of appropriate outsourcing arrangements should be structured in accordance with the three lines of defence model, involving direct operational responsibilities as well as senior management and Board oversight. Typically, the Compliance Manager (or similar role) would be responsible for ensuring that the firms' outsourcing arrangements comply with regulatory requirements (a second line of defence activity) and would be directly accountable to the Board (operating at the third-line of defence). Responsibilities would be documented in role specific job descriptions.

Outsourcing life cycle

The process of outsourcing should be undertaken in accordance with a defined outsourcing 'life cycle' which would comprise a number of distinct stages within which certain controls will be operated. The stages typically comprise:

- **Planning process** – planning whether it is appropriate to outsource a particular business function and how the firm would control the outsourced function. The development of a service description and associated service levels would take place at this stage.
- **Risk assessment** – assessing the risks associated with outsourcing a particular function and understanding how these risks would affect, and be controlled by, the firm. This would lead to approval in principle to outsource a particular function, provided that the associated risks are capable of control within the firms' risk appetite
- **Tendering process** – obtaining quotes for the proposed outsourced function from different service providers
- **Due diligence** – performing due diligence on potential service providers, leading to a short-list of suppliers or an initial choice of supplier
- **Contractual negotiations** – contractual negotiations regarding service delivery, regulatory and commercial requirements with the short-listed potential suppliers. This will lead to a choice of preferred supplier who is able to meet the firm's contractual requirements
- **Approval** – approval of the relationship with the final proposed service provider. The Board should have final approval authority and execute on the contractual agreement negotiated above
- **Implementation** – establishing the operational arrangements that will enable the outsourcing of the business function to the proposed service provider; and
- **Termination** – following conclusion of the outsourcing relationship the arrangements will need to be terminated, in accordance with contractual provisions, and an 'exit plan' initiated. Termination may take place if the service provider is not able to meet requirements (e.g. service levels), if the firm wishes to bring the function in house, or if the outsourced function is no longer required. Termination and exit planning would also feature in the firms' Wind Down Plan.

Summary of outsourcing arrangements

The use of outsourcing to facilitate the delivery of services by EMI / PI businesses is common and well understood by the FCA. However, for a firm to outsource key business functions it will need to ensure that certain regulatory requirements and guidance are met:

- the outsourcing arrangements do not impair the quality of internal control or the FCA's ability to monitor the firm
- the outsourcing arrangements do not result in the delegation of responsibility for complying with regulatory requirements
- the relationship and obligations of the firm towards its customers is not substantially altered
- compliance with conditions of authorisation are not altered; and
- no authorisation conditions require removal or variation.

Outsourcing policies and procedures should be maintained to address the areas detailed below and would be documented in both the Compliance Manual and the Outsourcing Policy; the Compliance Manual would typically describe the high-level approach (e.g. policies and summarised procedures) and the Outsourcing Policy would be used to document the details. The Outsourcing Policy would be referenced in the Compliance Manual as a supporting document.

The development of a Compliance Manual is addressed in ***Compliance Arrangements Guide 2: Developing a Compliance Manual***.

Outsourcing arrangements should include policies and procedures that address the following areas:

- **Service description** – the activities that will be outsourced should be defined in service descriptions, including service delivery metrics. Service descriptions would be based on the activities and responsibilities associated with the business function to be outsourced and will form the basis of the discussions to be held with prospective service providers, selection and due diligence of the service providers, and the monitoring of service provision. Service descriptions should be documented and approved by the Board.
- **Service provider due diligence** – a process will need to be developed in relation to the initial selection of service providers. On an ongoing basis the due diligence performed on service providers should be kept up to date as part of the ongoing monitoring arrangements. Commercially it makes sense to perform initial due diligence on service providers in order to select the best fit before outsourcing. For an authorised EMI / PI the initial due diligence performed on potential service providers should be a little more involved, going beyond answering commercial questions such as whether they can provide the services for a fair price and meet service levels. For example, whether the service provider be willing to sign up to contractual agreements that will meet regulatory requirements, including the provision of audit rights to the firm and the FCA. Ongoing monitoring of the outsourcing arrangements would include the monitoring of service delivery in line with the service description and associated service levels (as defined in the contractual agreement).
- **Contractual arrangements** – contractual agreements should be put in place between the firm and its service providers (including intra-group service providers). The contractual arrangement should include a clear service description and service levels as well as contractual terms such as audit rights for the firm and FCA, reporting requirements, data protection, security, termination rights, and handover rights.
- **Maintain a register of outsourcing arrangements** – firms should maintain a table of the outsourcing arrangements (or as the EBA Guidelines require, a 'Register') detailing information that can be used to support oversight and control activities, such as the service description, service provider name, location, the role assigned with oversight responsibility and contact points. EBA Guidelines detail the information that would be expected to be documented in an 'Outsourcing Register'.
- **Oversight arrangements** – the firm retains responsibility for all outsourced functions, this responsibility cannot be delegated. This necessitates the allocation of 'oversight' responsibility to an appropriate role within the business, typically the role that would have been responsible for the business function had it not been outsourced. The outsourced business function should be included in the staff organisation chart together with the reporting line to the oversight role.

- **Monitoring arrangements** – the delivery of outsourced services should be subject to ongoing monitoring (as part of the oversight arrangements) and the firms' outsourcing policies and procedures subject to ongoing review and development. Monitoring of a firms' approach to outsourcing would interact with other operations of the firm, e.g. the use of a Compliance Monitoring Programme and the Risk Register.
- **Management information reporting** – to support oversight of the outsourcing arrangements, management information should be provided through the functional reporting lines and, in particular, to the Board (at the third-line of defence) as part of the regular reporting information provided ahead of each Board meeting.

Service description

The activities that will be outsourced by the firm should be clearly documented in service descriptions, including service delivery metrics, with associated key performance indicators ("KPI"), as part of the 'Planning' stage of the outsourcing life-cycle. Service descriptions would be based on the activities and responsibilities associated with the business function to be outsourced and should be approved by the Board. Service descriptions would then be used as the basis for the 'Risk assessment' and 'Tendering stages' of the outsourcing life-cycle, as well as the 'Due diligence', 'Contractual negotiations' and 'Implementation' stages.

Service levels should form part of the service description in order to provide a benchmark for the measurement of the performance of the service provider. The service levels should define the service performance that the firm expects from the service provider and be agreed by the Board. KPIs would be used to monitor service delivery in accordance with the defined service levels. The majority of KPIs would be quantitative although qualitative performance indicators could also be used. The defined KPIs would be used by the firm to measure the quality of service delivery, performance of the service provider and be reported to the firm in accordance with contractual arrangements. The service provider should be held contractually liable to deliver the services in line with the service levels. If monitoring activities indicate that the services fall below the expected service levels, penalties could be levied in line with contractual terms.

The preparation of service descriptions that describe the activities that will be outsourced will require the firm to consider the responsibilities associated with the business function to be outsourced – the definition and allocation of responsibilities to roles and business functions is an important part of developing the staff organisation structure and the implementation of a three lines of defence model. Further guidance on these areas is provided in:

- ***Applications for Authorisation Guide 3: Staff organisation structure***
- ***Risk Management Arrangements Guide 4: Three lines of defence model***

Service provider due diligence

Firms should perform due diligence on the candidate service providers, as identified during the 'Tendering' stage of the life-cycle. The due diligence process would lead to the next stage of the life-cycle, the 'Contractual negotiations' stage; this stage could also form part of the due diligence process, i.e. if the firm and candidate service provider cannot reach an agreement on contractual terms the service provider should not be selected.

The due diligence process developed in relation to the initial selection of service providers should be documented and could be coordinated through the use of a due diligence checklist.

The due diligence performed as part of the selection process should be reviewed, and if necessary updated, on an ongoing basis as part of the ongoing monitoring of outsourcing arrangements. The ongoing monitoring of the outsourcing arrangements would include the monitoring of service delivery in line with the service description and associated service levels / KPIs – these should therefore be defined in the contractual agreement between the firm and service provider, together with rights of recourse for unsatisfactory service provision.

Contractual arrangements

Contractual agreements must be agreed and put in place between the firm and its outsourced service providers (both third-party and intra-group service providers) to govern the provision of the outsourced services – a key part of the contractual arrangements would therefore be the service description and the required service levels. The requirements of the contractual arrangements should be discussed during the 'Due diligence' stage of the outsourcing life-cycle and agreed during the 'Tendering' stage. The Board should have final approval of the contractual arrangements that are executed.

The contractual agreements governing the outsourcing arrangements would need to include terms covering a number of areas, including:

- A clear description of the outsourced function to be provided and the associated service levels required by the firm
- Start date and end date of the agreement and notice periods
- Governing law
- Financial obligations of the respective parties
- Whether the sub-outsourcing is permitted
- Provisions regarding the accessibility, availability, integrity, privacy and safety of data
- Rights to monitor the performance of the service provider on an ongoing basis
- Reporting obligations of the service provider and the scope and format of information
- Penalties in case of breach of contractual obligations
- Requirements to implement and test business contingency plans
- Provisions ensuring access to data and data protection
- The obligation of the service provider to cooperate with the competent authorities
- Rights of the firm and competent authorities to inspect and audit the service provider
- Termination rights; and
- Handover arrangements.

Register of outsourcing arrangements

A table, or 'Outsourcing Register', detailing relevant information should be maintained in accordance with the EBA Guidelines on outsourcing. The Outsourcing Register should include details of the outsourced services, service providers, contact points and key service levels, as well as other information defined in the EBA Guidelines. The Outsourcing Register would be used as a reference source when operating the compliance, risk management, internal audit and internal control procedures.

Oversight arrangements

The Board has responsibility for the oversight of the firm's operations and compliance with regulatory requirements, as a whole, including oversight of the outsourcing arrangements. The Board should receive management information that is appropriate to facilitate this oversight

responsibility (see below). Firms should also implement a three lines of defence model within the business, with responsibilities for risk management (which would include risks associated with outsourcing arrangements) being assigned to various roles within each of these levels. In accordance with a three lines of defence model, day-to-day oversight activities could be integrated within the business operations:

- the Board would exercise oversight of the business as a whole, including outsourcing arrangements and would receive management information from the second line of defence
- the Compliance Manager would oversee the regulatory compliance arrangements that apply to outsourcing, e.g. the Compliance Manual, Outsourcing Policy and arrangements documented therein. The Compliance Manager would use the Compliance Monitoring Programme ("CMP") as a key monitoring tool for regulatory compliance matters, including outsourcing.
- other second line of defence senior management roles would oversee specific outsourcing arrangements, e.g. the IT Manager would oversee outsourced IT functions, a Finance Manager would oversee outsourced finance activities, etc.
- first line of defence roles, i.e. operational roles, are unlikely to be involved in oversight activities since it is likely that their activities are the ones being outsourced. However, there may be instances where first line of defence roles contribute to the oversight exercised by second lines of defence roles.

Oversight responsibilities should be documented in the job descriptions for the relevant roles and be assigned in accordance with the staff organisation structure of the business. Firms should provide training to ensure that staff understand their responsibilities.

Monitoring arrangements

The oversight arrangements described above form part of the monitoring arrangements that firms will need to implement to ensure that outsourcing arrangements meet regulatory requirements. In addition to the oversight of the delivery of the outsourced services, the firm's overall approach to outsourcing, i.e. the policies and procedures that are maintained, should also be subject to ongoing development and review.

The ongoing monitoring of a firms' approach to outsourcing will interact with other compliance, governance and risk management operations of the firm, including the use of the Compliance Monitoring Programme ("CMP"), Risk Register and activities of the Internal Audit function. These activities will primarily be undertaken at the second line of defence, typically by the Compliance Manager.

Additional guidance on these areas is available:

- ***Compliance Arrangements Guide 3: Building a Compliance Monitoring Programme***
- ***Risk Management Arrangements Guide 2: Risk management framework***
- ***Risk Management Arrangements Guide 3: Building a Risk Register***
- ***Governance Arrangements Guide 3: Internal audit arrangements***

Management information reporting

The reporting of appropriate management information will be key to ensuring the effective oversight of the outsourced functions, the monitoring of the firm's outsourcing controls and the risk management activities. Information will need to be reported through the three lines of defence, i.e. from first to second to third.

The information reported to the second and third lines of defence should be appropriate to meet the activities being performed, for example, the Board will require reasonably high-level information on the outsourcing arrangements and the performance of service providers – this would involve reporting KPIs and key issues that have been identified.

Information reported to the second line of defence would need to be appropriate for the particular role being performed, e.g. the Compliance Manager would be concerned about whether regulatory requirements are being met whereas other second lines of defence would require information relevant to their oversight of specific outsourced functions, including information reported directly from the service provider in accordance with contractual requirements.

Further guidance on management information reporting is available: ***Governance Arrangements Guide 4: Management information reporting***.