payments and crypto network

Governance arrangements

A series of guides addressing the subject of governance arrangements for UK authorised Electronic Money Institutions ("EMI") and Payment Institutions ("PI").

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

Guide 1: Overview of governance 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 associated guidance from the UK's Financial Conduct Authority ("FCA").

The EMR and PSR require firms to maintain *"robust governance arrangements"*, including *"a clear organisational structure with well-defined, transparent and consistent lines of responsibility"*, which are *"comprehensive and proportionate to the nature, scale and complexity of electronic money to be issued and payment services to be provided".*

The requirement to maintain 'robust' governance arrangements will require a degree of interpretation considering the context of the particular firm. In any case, there are some key areas of governance that will be considered in this guide.

Summary of governance arrangements

An authorized EMI or PI must comply with a number of regulatory requirements, including maintaining robust governance arrangements which should include the following:

- **Board of Directors**: The board of directors ("Board") is responsible for the overall governance and strategic direction of the firm. The Board is accountable to the shareholders and must act in the best interests of the company.
- **Senior Management**: The senior management team is responsible for the day-to-day operations and management of the firm and is accountable to the Board.
- **Risk Management**: The EMI / PI must have in place robust enterprise-wide risk management systems and controls, which include procedures for identifying, assessing, mitigating and reporting risks that are relevant to the business.

- **Compliance arrangements**: The EMI / PI must have in place a compliance function, comprising at least one person) that is responsible for ensuring that the business complies with all relevant laws and regulations, including guidance published by the FCA.
- **Internal Audit**: An EMI / PI will need to consider how it will operate an internal audit function, that is independent of the rest of the organization, which is responsible for evaluating the effectiveness of the internal controls, risk management systems and governance arrangements. It is possible to outsource the internal audit function, in whole or part, to access 'independent' resources and suitable expertise to perform the function (this is common, particularly within smaller businesses).
- **Money laundering and terrorist financing**: An EMI / PI will need to have in place risk-based procedures and controls designed to prevent money laundering and terrorist financing. The firms' Money Laundering Reporting Officer ("MLRO") will be a key role maintained as part of these arrangements.

The governance arrangements in an EMI / PI should ensure sound, effective and compliant business operations and protect the interests of its customers and will need to be developed considering the specific context of the business.

A firms' governance arrangements would cover the activities of the three-lines of defence but would typically operate at the third, and to some extent the second, lines of defence.

Each of the above areas are described in a little more detail below.

Board of Directors

In the UK, the board of directors ("Board") is the highest level of decision-making body within a company. It is responsible for overseeing the management and direction of the company, setting strategic objectives and policies, and representing the interests of shareholders.

Within an EMI or PI business, the Board will hold ultimate responsibility for compliance with regulatory requirements as part of their general 'oversight' responsibility. Senior manager roles will support the Board from an operational perspective, e.g. key senior manager roles such as the Compliance Manager and MLRO will hold day-to-day operational responsibility and report to the Board.

The Board could comprise both Executive and Non-Executive Directors ("NED") with the former having day-to-day operational involvement in the business and the latter adding a governance layer to the business. Maintaining NED roles is not a requirement for an EMI / PI although appears to be increasingly encouraged by the FCA from a best practice perspective. Note that other regulators do have specific requirements for NEDs.

Also, there are no requirements for an EMI / PI to maintain specific directorship roles, although it would be logical to maintain a role to lead the business, e.g. Chief Executive Officer ("CEO"). Individuals performing directorship roles would need to be approved by the FCA as 'fit and proper', i.e. as an 'EMD / PSD Individual'. Decisions regarding the executive director roles to be maintained by a firm should be driven by operational and organisational requirements.

The Board should meet on a regular basis in order to exercise their responsibilities, i.e. business oversight and setting strategic direction, and in doing so consider reporting information provided (e.g. in a Board Reporting Pack), through the agreed reporting lines, by senior management.

Further guidance can be found in ***Governance Arrangements Guide 2: Board composition and responsibilities***.

Senior Management

Senior manager roles would be allocated with operational responsibilities and report to the Board. Senior manager responsibilities would essentially be delegated by the Board and should be documented in role specific job descriptions. The specific senior manager roles that would be maintained by an EMI / PI should consider the executive director roles that are maintained, for example, an EMI / PI might not maintain a Compliance Manager role as a senior manager if there is an executive director performing a Chief Compliance Officer role (unless the firm was a significant size); the business would need to consider whether the roles / resources would compliment each other rather than duplicate efforts. Individuals performing most senior management roles would also need to be approved by the FCA as 'fit and proper'.

Further guidance can be found in ***Applications for Authorisation Guide 3: Staff organisation structure***.

Risk Management

EMI and PI businesses must maintain adequate internal control mechanisms, including sound administrative, risk management and accounting procedures which are comprehensive and proportionate to the nature, scale and complexity of the business. The risk management arrangements should enable the EMI / PI to identify, manage, monitor and report any risks to which they might be exposed. The risk management arrangements are often referred to as a Risk Management Framework and should be considered as part of the governance arrangements operated by firms.

Further guidance on risk management arrangements can be found in:

- ***Risk Management Arrangements Guide 1: What is risk management?***
- ***Risk Management Arrangements Guide 2: Risk management framework***

Compliance arrangements

An EMI / PI will need to maintain arrangements that are designed to ensure compliance with applicable regulations, including the Electronic Money Regulations 2011 ("EMR") and Payment Service Regulations 2017 ("PSR"). Guidance will also need to be considered including guidance published by the FCA and European Banking Authority ("EBA").

Compliance arrangements include the systems, processes, and structures that are operated by an EMI / PI that are designed to ensure compliance with regulatory requirements and applicable guidance. 'Compliance' here relates to the arrangements maintained to meet the requirements of authorisation rather than the prevention on financial crime.

Policies and procedures would need to be developed, implemented and monitored and should be suitably documented, e.g. in a Compliance Manual. Monitoring of the compliance arrangements would typically be coordinated through the operation of a Compliance Monitoring Programme ("CMP"). Further guidance on these can be found in:

- ***Compliance Arrangements Guide 2: Developing a Compliance Manual***
- ***Compliance Arrangements Guide 3: Building a Compliance Monitoring Programme***

Responsibility for the firms' compliance arrangements will need to be allocated to a suitable role, e.g. Compliance Manager, performed by an individual with a suitable level of experience (who will need to be approved by the FCA as an EMD / PSD Individual).

Firms' should make a distinction between compliance arrangements that concern the FCA's conditions of authorisation as opposed to those designed to prevent financial crime (see below) – operationally it tends to be helpful to treat these as two separate and distinct areas.

Money laundering and terrorist financing controls

EMI / PI businesses must implement risk-based controls to prevent financial crime, i.e. anti-money laundering ("AML") and counter terrorist financing ("CTF") controls. Financial crime controls must cover a number of different areas, including:

- Customer due diligence measures (i.e. identifying and verifying the identity of customers)
- Monitoring transactions for suspicious activity
- Reporting suspicious transactions within the business and to the relevant authorities
- Sanctions screening; and
- Checking for politically exposed persons ("PEP").

Responsibility for the implementation and operation of risk-based financial crime controls resides with the Board who would typically allocate day-to-day responsibility to the Money Laundering Reporting Officer ("MLRO"). The responsibilities of the MLRO should be clearly documented in a job description for the role.

In a similar manner to the regulatory compliance arrangements (as described above), the risk-based financial crime controls would be defined in a set of policies and procedures and be suitably documented, e.g. in an AML Manual. The ongoing monitoring of the AML / CTF arrangements would typically also be coordinated through the operation of the Compliance Monitoring Programme.

Internal Audit

The internal audit function should work, in an independent manner, to assess and improve the effectiveness of the firms' risk management, control, and governance processes and report to the Board or a suitable Board-level committee, e.g. Audit committee (if one is maintained). The internal audit function could be outsourced by an EMI / PI in order to ensure independence and access to suitable resources and expertise. The internal audit function would work from an Internal Audit Plan which should detail the various audit areas that will be within the scope of each audit visit and their respective frequency of review. The use of group or external internal audit resources is often implemented on an outsourced basis.

Further guidance on these can be found in:

- ***Governance Arrangements Guide 3 - Internal audit arrangements***

Management information reporting

Management information should be reported to the Board for a number of reasons:

- **Governance**: The Board is responsible for oversight of the business and management information will be necessary to fulfil this responsibility.
- **Decision-making**: Management information is essential for the Board to make appropriate decisions regarding the operation of the business and its strategic direction.
- **Performance evaluation**: Management information would be used to evaluate the performance of the company and its management team.
- **Compliance and financial crime**: In order to ensure the EMI / PI complies with applicable regulations and guidance, appropriate compliance and financial crime related management information will need to be provided.
- **Risk management**: Risk management information, typically produced using the Risk Register, would be used to facilitate the Boards' ability to oversee risk within the business.
- **Strategic planning**: Management information should be used to inform the development of the company's business and strategic plans, including financial forecasting activities.

The types of management information reported to the Board of an EMI / PI could therefore include:

- **Financial performance** – actual results compared to budget with explanations of significant variances. Typical financial performance metrics could be used which should also cover regulatory capital requirements and measures of 'adequate financial resources' (think Wind Down Planning).
- **Business development –** updates on business development activities, client onboarding metrics, developments / integrations with potential partners, sales pipeline, customer feedback, updates on service and functionality development and launch plans and licensing matters.
- **Compliance arrangements** – updates on matters relating to compliance with applicable regulations and guidance. New policies or changes to existing policies should be highlighted for approval by the Board. Output from the Compliance Monitoring Programme ("CMP") and compliance reviews, or internal audit, could be incorporated into the reporting information as well as forward looking analysis of changes in the regulatory environment that may affect the firm. This section should be the platform through which the Compliance Manger (or similar role) can raise issues or concerns.
- **Financial crime** – including updates in the AML / CTF arrangements, new policies or changes to existing policies for approval by the Board, suspicious activity and external reporting metrics. As above, output from CMP, compliance reviews and internal audit activities may be helpful for preparing financial crime related reporting information. Forward looking analysis of changes in the regulatory environment should also be highlighted. This section should be the platform through which the MLRO can raise issues or concerns.
- **Risk management** – risk reporting information could be derived from the Risk Register and presented in a 'dashboard' format to enable the Board to gain an understanding of the current risk environment. The 'dashboard' would be a condensed version of the Risk Register. Additional, more granular, detail could be provided in relation to risks

that are assessed as being 'high' together with recommended risk reduction actions for which the Board should be aware or provide approval.

- **Complaints and disputes** – metrics relating to complaints received and disputes resolved together with information on root causes (i.e. root cause analysis) and recommended improvements.
- **Strategic planning** – this might include updates on the strategy of the business, changes to the markets in which the EMI / PI operates and information on competition. This information would likely come from the CEO and other Board members.
- **Cybersecurity** – details of security incidents, work undertaken to improve security and recommended actions for consideration / approval. Reporting from the IT Manager (or similar role) and Information Security Officer ("ISO") would be provided here.

Further guidance on these can be found in:

- ***Governance Arrangements Guide 4 - Management information reporting***

Three lines of defence model

The three lines of defence model is a risk management approach that divides the responsibility for managing risks into three distinct categories. As mentioned above, risk management should be considered as part of the overall governance arrangements.

In summary, the three lines of defence approach, from a governance perspective, would comprise:

1. **Operational risk management**: This is the first line of defence and refers to the front-line activities and processes that are in place to identify, assess, and manage risks. Typically taking place in the operational business functions.
2. **Risk oversight**: This is the second line of defence and involves the independent oversight of risk management activities at the first line of defence, comprising activities such as monitoring and testing, reporting, and advice and guidance. Typically, being performed by senior management roles using tools such as the Risk Register and CMP.
3. **Assurance and audit**: This is the third line of defence and involves the independent evaluation of the effectiveness of the first and second lines of defence, including the activities of internal audit, external audit, the Board and Board-level committees. The reporting of management information from the second line to the third line is critical for this to take place.

The three lines of defence model is designed to ensure that risks are identified and managed in an effective manner across the business, i.e. that the Risk Management Framework operates to manage risk on an enterprise-wide basis.

Further guidance on these can be found in:

- ***Risk Management Arrangements Guide 4 - Three lines of defence model***

In summary, the governance arrangements that are maintained by an EMI / PI will impact a number of different areas, and utilise a number of different approaches. They will need to be developed considering the specific context of the firm and kept under review as the business develops. The operation of effective governance arrangements should also benefit the

business from an operational perspective, increasing efficiencies and maximising opportunities.