payments and crypto network

Preparing an Application for Authorisation

A series of guides addressing common issues in relation to preparing an application for authorisation.

Guide 6: Risk management arrangements

Background

Electronic Money Institutions ("EMI") and Payment Institutions ("PI") are required to maintain risk management arrangements that identify, manage, monitor and report any risks to which they might be exposed. These arrangements do not necessarily involve the operation of a separate risk management function but must be 'effective', essentially that they are proportionate to the nature, scale complexity of the firm's activities. The application for authorisation will need to describe, in reasonable detail, how the risk management activities are structured and performed. This guide should help you develop a risk management approach that can be described in your application and operated on an ongoing basis.

Scope of the risk management activities

Risk management should be performed on an enterprise-wide basis. There is a common misconception that the focus of risk management is financial crime or fraud - these are certainly within the scope of risk management but will need to be considered alongside many other areas of the business.

Risk categories should be used to organise risks - the FCA published guidance refers to the following categories: settlement risk, operational risk, counter-party risk, liquidity risk, market risk, financial crime risk and foreign exchange risk. You might want to use these risk categories as a starting point. The use of sub-categories would also make sense, for example, financial crime risk could be analysed into sub-categories that include: customer type, delivery channel, geographies, service functionality etc.

The risk management arrangements should also be operated across all three-lines of defence:

- First line of defence risk management activities take place as part of the daily activities of the respective business functions. Responsibility for assessing / monitoring individual risks could therefore be assigned to staff / roles at this level.

- Second line of defence would typically involve the activities of senior staff responsible for risk, e.g. the Compliance Manager and MLRO roles.
- Third line controls would comprise the activities of the Board and any Internal Audit activities (the latter not being compulsory but increasingly difficult to avoid). Board level committees, if maintained, would also be considered here.

Information will need to be reported between these three lines to facilitate a coherent enterprise-wide approach that can operate effectively as the business and environment change over time.

Responsibility for risk management

A clearly defined approach to risk management will need to be adopted and the allocation of risk management responsibilities will be key. Responsibilities could be allocated across the three lines of defence; a second line of defence role would typically be responsible for coordinating the day-to-day operation of risk management activities – very often the Compliance Manager (although the MLRO role would typically have responsibility for coordinating AML / CTF risk management).

Responsibilities should be set out in role specific job descriptions and appropriate training provided. Roles operating at the first line of defence will need to be aware that they have a responsibility to support the process of identifying risks and associated mitigating controls (reporting them to the second line of defence for assessment and recording).

Risk appetite

How much risk is too much risk? How far should risk be reduced? The answer will depend on the 'risk appetite' of the business.

The objective of risk management is to direct resources towards the riskier areas of the business in order to reduce the risks to an acceptable level - risk management is about managing risks rather than eliminating them altogether! The level of risk that is acceptable for the business is referred to as its 'risk appetite'.

The risk appetite of the business should be set by the Board. The risk appetite could vary by risk category, e.g. the risk appetite for regulatory risks might be set as 'Low' whereas the appetite for operational risks could be 'Medium' - this might be appropriate for a new business or a business addressing new markets (i.e. the business cannot be too conservative / cautious).

Risks and Mitigating controls

Risks may be identified across all three lines of defence, although the majority of risks are likely to originate at the first line of defence, i.e. being operational in nature. Risks identified at the second and third lines of defence are likely to be wider in scope or relate to external factors. As mentioned above, it is therefore important that staff within each level understand the importance of managing risk and the individual contributions that they can make by identifying and reporting risk.

Mitigating controls serve to manage risks, these will also need to be identified alongside the risks themselves. Mitigating controls may already exist within the business, being operated to

mitigate known risks, or may need to be developed. Detailed knowledge of the risk will be required in order to develop appropriate mitigating controls.

The ability to separately assess risks and their associated mitigating controls is key to an effective risk management framework. It should also help identify improvements in resource allocation / operational efficiencies, for example, a risk may reduce over time due to changes in the business or environment and, in this event, the associated mitigating controls (if considered separately) could also be reduced, thus freeing resources for allocation elsewhere in the business.

Risk assessments

Assessments of the risks, and the effectiveness of their associated mitigating controls, will need to be undertaken on an ongoing basis. The frequency of these assessments will depend on the severity of the particular risk, as determined from the latest assessment. Risks that are assessed as the most severe should be addressed first; that is, the firm's resources should be allocated towards implementing and operating mitigating controls that reduce the severity of the risk.

Rewinding a little; mitigation of a risk is one course of action that a firm can take if the risk assessment exceeds the designated risk appetite. Other courses of action are also possible where the risk appetite is exceeded:

- Avoidance – this would involve a change in the business, services, operations, etc. in order to avoid the risk altogether. If 'Avoided', the risk would no longer be applicable to the firm; and
- Transference – the root cause of the risk would be transferred to another party, e.g. through the use of outsourcing arrangements or the purchase of insurance.

A fourth course of action would be Acceptance, but only where the risk is already below the risk appetite of the firm.

Risks, and the effectiveness of mitigating controls to address those risks, should both be recorded and assessed. The assessment of the risk, in its raw form before mitigating controls are applied, would be referred to as the 'Inherent' risk. When the effectiveness of the mitigating controls are assessed, and combined with the Inherent risk, the risk that remains within the business is the 'Residual' risk.

So, if Inherent risk is beyond the risk appetite the firm will need to Avoid, Transfer or Mitigate the risk. If the risk is Avoided or Transferred it would not need Mitigating and would no longer need to be tracked. If, following the application of the mitigating controls the Residual risk still remains above the risk appetite, further action will be required, e.g. strengthened mitigating controls (or perhaps now a decision to Avoid or Transfer).

Risk Register

The management of risk is a continuous process and requires reasonable effort to organise and operate on an ongoing basis. It is usual to maintain a Risk Register, to facilitate this effort, as the key operational 'tool' used to record risks, mitigating controls, assessments and to produce risk management information. Without the use of a Risk Register it will be very difficult to record and collate the necessary information.

The Risk Register would record the risks that are relevant to the business, i.e. not those that have been Avoided or Transferred. Risks that have been Accepted should be recorded since they may change over time and potentially exceed the risk appetite (and therefore require a risk treatment).

Risk reporting information

Key to the operation of an effective risk management framework will be the reporting of risk information between the three lines of defence. Typically, the first line of defence (operational in nature) would report to the second line of defence (e.g. the EMD Individual role that has responsibility for risk management). The second line of defence role would work with the first line of defence (operational business functions) to manage the enterprise-wide risks and report to the third line of defence, i.e. the Board (and any Board-level Committees that are maintained). Within the context of a larger group, risk reporting information may also be provided to group audiences (e.g. a group risk function or committee).

The reporting of risk management information to the Board will be key to ensuring that the firm addresses risk in an appropriate manner; it is the Board that will ultimately approve the allocation of resources to the management of risk (in line with their ultimate responsibility as directors of the company). The Board Pack provided to the Board ahead of each Board meeting should include a dedicated section on risk so that the necessary management information is provided on a regular basis.

Risk reporting information could be generated from the Risk Register, for example, producing a risk 'dashboard' for inclusion in the Board Pack. The Risk Register should be considered a key source of risk information.

What do we need to describe in an application for authorisation?

As referenced in the current FCA application form, an application for authorisation requires the submission of a 'risk mapping' that describes the types of risk and the procedures that will be been put in place to assess and prevent those risks. This could take the form of a table, summarising risks for each risk category and a summary of the associated mitigating controls, at a high level; essentially a highly summarised version of the risk register.

Should the application just include a 'risk mapping' table? No.

Regulations require firms to have adequate internal control mechanisms, including risk management, which are comprehensive and proportionate to the nature, scale and complexity of the business. The application content should therefore describe the approach adopted by the firm in sufficient detail to enable the FCA to assess whether this requirement will be met.

The focus of the descriptions should be the enterprise-wide risk management framework applied throughout the business (which would also include financial crime, e.g. having 'financial crime' as a distinct risk category). *Note: on the subject of financial crime, the application would also need to describe the financial crime risk assessment (upon which the risk-based financial crime policies and procedures should be developed).*

Risk management is a theme that should be woven into the entire application, in a similar manner to the concept of the three-lines of defence approach. For example, risk management activities should feature in your governance, internal control, financial crime, safeguarding,

financial forecasting, stress testing, IT and capital requirements descriptions that are provided in the application.

Applicant firms are often tempted to submit a copy of their Risk Register with the application for authorisation. I would not recommend this, rather focusing on the risk mapping summary and a comprehensive description of the risk management arrangements operated by the firm.

Importantly, following submission of the application, any work that can be performed to implement the described risk management approach will assist the firm respond to the FCA's questions (that will inevitably be raised during their assessment of the application).