payments and crypto network

Risk management arrangements

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

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

Guide 2: Risk management framework

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").

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".

Composition of a Risk Management Framework

A Risk Management Framework would typically comprise the following:

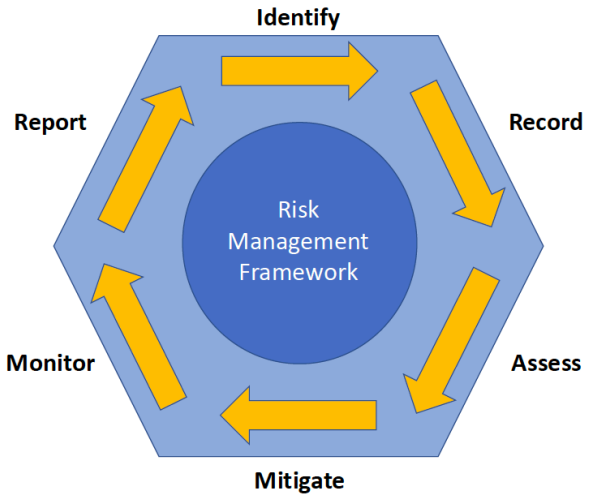
- **Policies** – risk management policies should be agreed by the Board and be documented in a suitable location. The firm's Compliance Manual is a logical place to include some risk management policies. It may also be appropriate to maintain a separate Risk Management Policy with a greater level of detail than would be included in a Compliance Manual. It would be for the firm to decide how it chooses to organise / document its risk management policies. The subject of developing a Compliance Manual is addressed in a separate guidance document: ***Compliance Arrangements: Guide 2 - Developing a Compliance Manual***.
- **Procedures** – risk management procedures will need to be operated in order to implement the agreed policies. Risk management procedures would also be documented in a similar way to the risk management policies, e.g. using a Compliance

Manual and / or Risk Management Policy document. A hierarchy of documents is logical, easier to update and helps to minimise duplication.

- **Responsibilities** – the day-to-day responsibility for risk management would typically be assigned to a role within the 'second-line of defence'. Risk management responsibilities should be documented in the job description associated with the role. Specific risk management responsibilities may also be associated with other roles, including Board-level roles, and would also be referenced in their job descriptions. Job descriptions should be approved by the Board.
- **Risk Register** – the key tool used in the management of risk. The Risk Register would be the primary document in the Risk Management Framework. The subject of building a Risk Register is addressed in a separate guidance document: ***Risk Management Arrangements: Guide 3 - Building a Risk Register***.
- **Business Continuity Plan** / **Disaster Recovery Plan** – the firms' BCP / DRP form part of the risk management arrangements of the business. Business continuity and disaster recovery planning are processes that serve to reduce risk and are therefore important risk mitigation activities.
- **Wind Down Plan** – the wind down planning process will consider risks that may lead to a wind down decision being made and define how the firm would react to such risks. Monitoring parameters would be defined as part of the wind down planning process and be integrated into day-to-day operations. In a similar manner to BCP and DRP, wind down planning is an important risk mitigation activity.
- **Board Reporting** – risk reporting information will need to be provided to the Board, to the FCA and potentially to group and/or external audiences. The format of the reporting information, e.g. a Board Reporting Pack for provision to the directors ahead of regular Board meetings, would therefore also be within the scope of the Risk Management Framework.

<u>Risk Management Framework stages</u>

Risk Management Frameworks would adopt a similar approach to managing risks, involving a number of distinct stages as illustrated in the diagram below. Different terms could be used to describe these separate stages but the process, and objective of each stage, would essentially be the same.



- **Identify** - Firstly, risks must be identified so they can be managed. Unidentified risks cannot be managed and will continue to pose a danger to the business.
    - If the process of identifying risks is unreliable the whole risk management process will be ineffective.
    - Staff should receive training to ensure that they are aware of the risk management process and the importance of identifying and reporting risks.
    - Risks might be identified through routine business operations or the performance of specific reviews / investigations. The majority of risks will likely originate within the first line of defence (i.e. the operational business functions).
- **Record** - Identified risks should be recorded in the Risk Register.
    - Risk that are recorded in the Risk Register will be within the scope of the Risk Management Framework and can then be assessed, mitigated, monitored and reported.
    - The information that is recorded for each risk should include a description of the risk and its assessment, the risk owner, a description of the mitigating controls applied and the residual risk that remains.
- **Assess** - Each risk should be assessed to establish its severity and to prioritise it for treatment.
    - Resources, whether financial or human, will be required to control a risk; it is therefore unlikely that a business would be able to control all of the risks that it faces (given that it will not have unlimited resources).
    - Businesses will therefore tend to accept some risks in order to operate. Risks will need to be prioritized, through the assessment process, so that resources can be directed to the most severe risks first.
    - The assessment process will need to be ongoing since each risk, as well as the wider 'risk environment', will potentially change over time.

- **Mitigate** - Risks will then be scheduled for mitigation depending on their priority. Mitigation requires some form of action to be taken. Action would involve Avoiding, Transferring or Mitigating the risk. If risks are not too severe they could be accepted. If a risk is Avoided or Transferred it could be removed from the Risk Register since it will no longer require management.
    - In order to have the greatest impact, the limited resources available to the business should be directed to the most severe risks first.
    - Risks can be treated (or Mitigated) in two ways:
        - Changing the nature of the risk itself such that its assessment reduces – e.g. changing the nature of the services offered, types of customers or markets addressed; and / or
        - Developing new, or reinforcing existing, mitigating controls. This will require resources to be directed to manage the risk.

- **Monitor** - The assessment of each risk and the effectiveness of the mitigating controls that have been applied to it will then need to be monitored. Risks that have been

Accepted would also be monitored in case their severity increases and they need to be managed.

- The risks and their associated mitigating controls will change over time – monitoring of the nature of the risk, the risk assessments and the mitigating controls will therefore be required on an ongoing basis.
- Monitoring should involve:
  - The Risk Owner periodically checking that the risk still exists in the manner recorded in the Risk Register (i.e. that the nature of the risk has not changed)
  - The review and update of the assessment of the risk; and
  - The review and update of the description and the effectiveness of the mitigating controls.

The use of the Risk Register will be key to the process of monitoring risks and recording the actions performed and the latest assessments.

- **Report -** Reporting information should be provided to those who are responsible for risk management, e.g. the Board (and any relevant Committees), department heads, etc., to facilitate their oversight activities.
  - In the case of the Board, risk information should be reported as part of the management information that is provided ahead of each Board meeting. The information should be sufficient to facilitate the management of the business, for example, highlighting areas where risks remain high and where additional resources should be directed.