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 4: Three lines of defence model

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") and relevant EBA Guidelines.

EMI and PI businesses must maintain risk management arrangements that enable the firm to identify, manage, monitor and report any risks to which it might be exposed.

EBA Guidelines, which also apply to UK authorised EMI and PI businesses, introduce the concept of a three-lines of defence model which should be considered when developing a firms' Risk Management Framework.

Description of the 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: operational risk management, risk oversight, and assurance and audit.

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. The majority of risks would originate from the first line operational business functions where there should be strong processes in place to ensure that risks are identified and managed.
2. **Risk oversight**: This is the second line of defence and involves the independent oversight of risk management activities performed at the first line of defence. This includes activities such as risk assessments, monitoring, reporting, advice and guidance. Roles such as the Compliance Manager, MLRO, Risk Manager, etc. would operate at the second line of defence. The Risk Register would also be operated at

the second line of defence in order to co-ordinate the risk management activities and the reporting of risk information to the third line of defence.

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. This includes activities such as internal audit, external audit, the activities of the Board and Board-level committees (if maintained).

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

Brief overview of the purpose and benefits of the three lines of defence model

The purpose of the three lines of defence model is to provide a systematic approach for managing risks within an organization, ensuring that responsibilities are allocated throughout the business in accordance with three distinct categories.

The benefits of using a three lines of defence model include:

1. **Improved risk identification and assessment**: By dividing the responsibility for managing risks into three distinct categories, it can help ensure that risks are identified and assessed more thoroughly and consistently within the business.
2. **Enhanced risk management**: By having multiple layers of defence, it can help ensure that risks are managed effectively, and that appropriate controls and mitigating measures are in place, throughout the business.
3. **Improved accountability and transparency**: By having clear roles and responsibilities for managing risks within each line of defence, it can help improve accountability and transparency within the organization.
4. **Enhanced confidence and assurance**: By providing, at the third line of defence, independent oversight and evaluation of the risk management activities, it can help build confidence and assurance in the effectiveness of the Risk Management Framework.
5. **Better decision making**: The systematic approach for managing risks that is fostered by the three lines of defence model can help strengthen decision making activities throughout the business and, in particular, at the third-line of defence.

First Line of Defence: Operational Risk Management

The first line of defence refers to the front-line activities and processes that are in place to identify, assess, and manage risks. These activities are typically carried out by business functions that are directly responsible for operational activities and which would be ‘close’ to the risks and mitigating controls (i.e. they should have a good understanding of their causes, nature, etc.).

Examples of risk management activities at the first line of defence include:

- Providing training and awareness programs to help employees understand their risk management responsibilities
- Operating processes to ensure that risks are identified as well as assessed in accordance with the defined risk assessment process
- Developing and implementing operational controls to mitigate risks

- Working with the second line of defence roles to facilitate the operation of the Risk Management Framework; and
- Implementing controls and systems to prevent, detect, and correct deviations from established policies and procedures.

The first line of defence is responsible for identifying and managing risks on a day-to-day basis, and for implementing controls and mitigating measures to reduce the 'Likelihood' or 'Impact' of risks.

Second Line of Defence: Risk Oversight

The second line of defence involves the oversight of risk management activities performed at the first line of defence and the maintenance and development of the Risk Management Framework as a whole. Activities such as monitoring and testing, reporting, and advice and guidance will be performed by roles such as the Compliance Manager, MLRO and/or Risk Manager operating at the second line of defence.

Examples of risk oversight activities at the second line of defence include:

- Monitoring and testing the effectiveness of controls and risk management processes at the first line of defence
- Providing guidance and support to the first line of defence regarding the Risk Management Framework
- Reporting on the effectiveness of risk management activities to the Board, i.e. the provision of risk management information on a regular basis (e.g. as part of a 'Board Reporting Pack' provided ahead of each Board meeting) and, where required, on an ad-hoc basis; and
- Facilitating the activities of the internal and external audit functions (third line of defence activities).

The second line of defence plays an important role in providing oversight and assurance that risks are being managed in an effective manner within the business.

Third Line of Defence: Assurance and Audit

The third line of defence involves the independent evaluation of the effectiveness of the first and second lines of defence. This includes activities such as internal audit, external audit and the oversight activities of the Board. The third line of defence should provide an objective and unbiased assessment of the firms' risk management arrangements.

Examples of activities at the third line of defence include:

- Board oversight of the risk management arrangements through consideration of management information provided by the second line of defence.
- Conducting internal audits to evaluate the effectiveness of the Risk Management Framework
- Engaging external auditors to provide independent assessments of the Risk Management Framework; and
- Managing enterprise level / strategic risks and developing strategies to mitigate them.

The third line of defence should provide a layer of independent assurance and help to ensure that risks are being managed in an effective manner across the organization.

Importance of the three lines of defence model

The three lines of defence model should help to ensure that risks are identified, assessed, and managed in an effective manner across the business – ‘effective’ in this context could mean in a thorough and efficient manner. It should also help to ensure that there is a clear division of responsibility for risk management, which can help prevent confusion and ensure that risks are identified, assessed and mitigated in an effective manner. The three lines of defence model should also help to foster a culture of risk awareness and risk management throughout a business, further supporting an effective risk management process and the ‘bottom-up’ reporting of risk information.

Potential challenges in implementing a three lines of defence model

The three lines of defence model is a structure that is often implemented in an intuitive manner, i.e. firms may already be operating it to some extent having organically developed the business. However, in formalising the approach, firms may face a number of potential challenges when implementing a three lines of defence model:

1. **Ensuring clear roles and responsibilities**: It is important to clearly define the roles and responsibilities of each line of defence in order to ensure that there is no unwanted / undefined overlap or gaps in coverage. This can be particularly challenging in large organizations with complex structures. Responsibilities will need to be clearly allocated to specific roles within each line of defence (reflecting them in associated job descriptions).
2. **Ensuring independence of the second and third lines of defence**: The second and third lines of defence should, as far as possible given the size of the business, be independent in order to provide objective assurance and oversight. This can be challenging, especially if there are close relationships or dependencies between them.
3. **Ensuring effective communication**: Effective communication is crucial for the three lines of defence model to work. It is important to establish clear channels of communication between the different lines of defence, as well as between any risk management function and the rest of the business. A clear organisational structure with defined reporting lines between roles and business functions is key.
4. **Managing cultural change**: Providing training and awareness to help employees understand their responsibilities with regard to risk management and implementing a culture of risk management where there has not been one previously.
5. **Ensuring adequate resources**: Establishing a three lines of defence model can be resource-intensive, as it requires the development of new processes, procedures, and systems. It is important to ensure that there are sufficient resources available to support the implementation and successful operation of the model. However, the structure and discipline that the model brings should more than justify the expense and inconvenience!