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 1: What is risk management?

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 are required to 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. These arrangements do not necessarily involve the operation of a separate risk management function but must be 'effective'.

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"). Aspects of the risk management arrangements will touch on some of the areas covered by the EBA Guidelines.

What is risk management?

Risk management is the process of identifying, assessing, and controlling threats to an organization. These threats, also known as risks, could come in the form of financial uncertainty, legal liabilities, operational disruptions, reputational damage, or strategic misalignment.

The objective of risk management is to minimize the impact of negative events on an organization and maximize the likelihood of positive outcomes. It involves creating a plan to identify and prioritize risks, assessing their likelihood and potential impact, and implementing strategies to manage or mitigate them.

There are several approaches (or 'treatments') that can be used to manage risks, including risk avoidance, risk reduction, risk transfer, and risk acceptance. The type of treatment applied to a particular risk would be guided by factors including the severity of the risk and the particular 'risk appetite' of the business.

Firms typically use a 'Risk Register', as a central risk management tool, to help coordinate their risk management activities and produce helpful management information.

What is risk appetite?

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

Risk appetite is the level of risk that a business is willing to accept in pursuit of a desired reward, e.g. achieving its strategic goals. It is a measure of how much uncertainty a business would tolerate in pursuit of a particular goal. Risk appetites can vary greatly between different businesses, as well as between the different risk areas within a specific business.

A 'high' risk appetite would indicate that the management of a business are willing to take on significant levels of risk in order to achieve their objectives. This could be a willingness to take on risk across the business as a whole or within certain areas of the business.

In managing risks, a business would seek to first direct resources towards the riskier areas in order to reduce them to an acceptable level. Since resources will inevitably be limited, businesses will need to prioritise where they are directed. 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.

Why is risk management important?

Risk management is a regulatory requirement for a UK authorised EMI or PI. The risk management arrangements must be both comprehensive and proportionate to the nature, scale and complexity of the EMI / PI business.

In general, risk management arrangements should help the business to identify and assess potential risks and take appropriate steps to mitigate or manage those risks. By identifying potential risks and taking proactive steps to address them, the likelihood of negative outcomes, such as financial losses or reputational damage, can be reduced.

Responsibility for risk management

Responsibility for the maintenance and operation of the risk management arrangements within an EMI / PI would typically be allocated to the role that is responsible for ensuring compliance with regulatory requirements. This day-to-day responsibility for risk management is in addition to the overall responsibility of the Board to ensure that the business complies with applicable legislation.

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 the AML / CTF risk management activities).

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).

What types of risks need to be managed?

The scope of the risk management arrangements should be ‘enterprise-wide’, i.e. cover all areas of the business from which risks may originate. 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; 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, to the extent that they apply to your business. Additional risk categories are also likely to be required, including:

- Financial risks
- Legal risks
- Reputational risks; and
- Strategic risks.

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. Sub-categories can be used to further assist risk management activities. The risk categories, and sub-categories, would be used as the basis for organising risks in the Risk Register and the provision of reporting information.

What does the risk management process involve?

An effective risk management process will need to involve a number of distinct stages, comprising, as a minimum:

- **Identifying risks** – processes will need to be operated that ensure risks are identified. These may be risks that already exist within the business or new risks associated with changes that the business is contemplating. Existing mitigating controls should also be identified at this stage. The majority of risks are likely to be identified at the first line of defence. Risks should be reviewed on a periodic basis since they are likely to change in nature over time.
- **Assessing risks** - assessments of the risks, and the effectiveness of their associated mitigating controls, will need to be undertaken on an ongoing basis. Assessments of the ‘Inherent Risk’ (before the application of mitigating controls) and the ‘Residual Risk’ (after the application of mitigating controls) should be performed. Risk assessments should also be reviewed on an ongoing basis to account for changes.

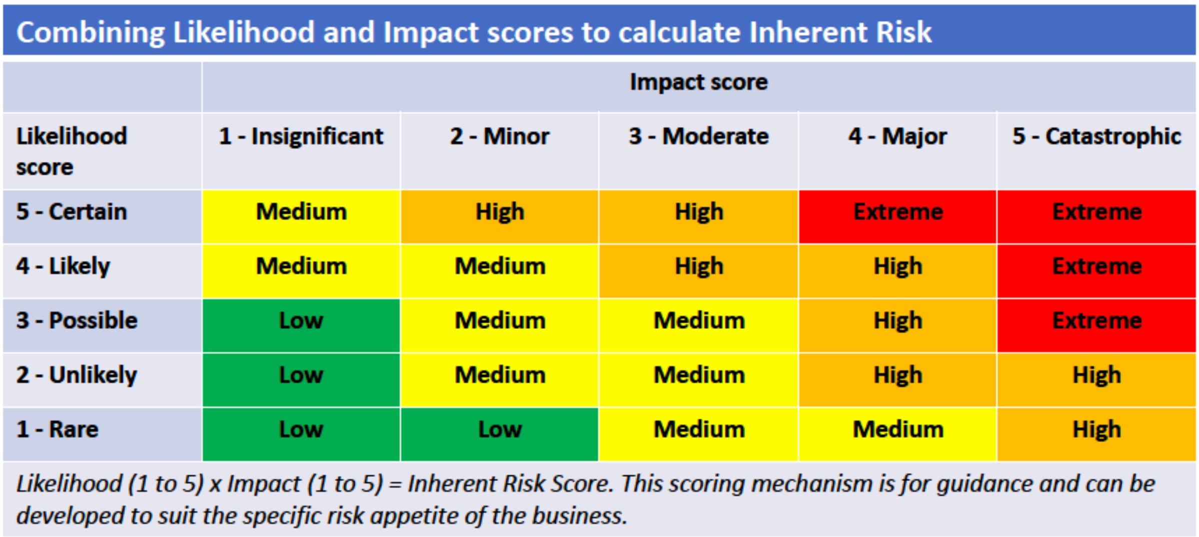
- **Managing risks** – risks would be prioritised for management according to their severity. The objective of the risk management process is to reduce risk rather than eliminate risk altogether. Resources, which will be limited, will therefore need to be allocated to the most severe risks first; and
- **Monitoring and reviewing risks** – the risk management process is a continual one and will need to ensure that risks, their assessments and the way in which they are managed are subject to periodic review.

How should risks be assessed?

Risks should be assessed in terms of their:

- **Inherent Risk** – an assessment of the risk before the application of mitigating controls. The inherent risk score would be used to prioritise the risks for treatment: the higher the inherent risk score the more urgently the risk should be treated; and
- **Residual Risk** – an assessment of the risk that remains after the application of mitigating controls. This will give an insight into the effectiveness of the mitigating controls that have been applied to reduce the inherent risk.

Risks would be assessed in terms of their Impact (i.e. if they occurred) and Likelihood (i.e. the probability of the risk occurring) and scores between 1 and 5 allocated to each. These Impact and Likelihood scores would be combined to calculate the overall risk score (see example table below).



Combining Likelihood and Impact scores to calculate Inherent Risk

	Impact score				
Likelihood score	**1 - Insignificant**	**2 - Minor**	**3 - Moderate**	**4 - Major**	**5 - Catastrophic**
5 - Certain	Medium	High	High	Extreme	Extreme
4 - Likely	Medium	Medium	High	High	Extreme
3 - Possible	Low	Medium	Medium	High	Extreme
2 - Unlikely	Low	Medium	Medium	High	High
1 - Rare	Low	Low	Medium	Medium	High

Likelihood (1 to 5) x Impact (1 to 5) = Inherent Risk Score. This scoring mechanism is for guidance and can be developed to suit the specific risk appetite of the business.

Based on the inherent risk score each risk can be categorised as either Extreme, High, Medium or Low. Prioritisation of risks for treatment would start with Extreme risks then those that are High risk, Medium risk, etc. until risks that exceed the Risk Appetite have all been appropriately addressed.

How are risks managed?

Following the assessment stage, risks will need to be managed (or 'treated') in accordance with their prioritisation (using the Inherent Risk Score) and with reference to the risk appetite of the business. Risks are typically treated in one of the following ways:

- Risk avoidance
- Risk reduction
- Risk transfer; or
- Risk acceptance.

If the Inherent Risk Score for a risk is below the Risk Appetite it can be Accepted – no further action required.

If the Inherent Risk Score for a risk is in excess of the Risk Appetite the risk could be:

- Avoided – 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; or
- Transferred – 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.

The remaining option, risk reduction involves taking steps to manage the risk, through the application of mitigating controls, to reduce the risk to within the Risk Appetite of the business, i.e. to reduce the Residual Risk to be below the Risk Appetite.

Three-lines of defence model

The risk management arrangements should be operated in accordance with the three-lines of defence model:

- **First line of defence** risk management activities take place as part of the daily activities of the respective operational business functions. Responsibility for identifying, assessing and 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. The operation of the Risk Register would take place at the second line of defence.
- **Third line of defence**, comprising the activities of the Board and Internal Audit. Board level committees, if maintained, would also be considered here. Management information would be reported from the second line of defence to enable the oversight responsibility held by the third line of defence.

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 changes over time.

What is a 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 (and certainly useful) 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 and produce reporting information for the third line of defence.

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 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. to the 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 meeting should include a dedicated section on risk so that the necessary management information is provided, and considered, 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.