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 3: Building a Risk Register

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. The risk management arrangements operated by a firm are referred to as a Risk Management Framework and a Risk Register operates as a central tool within that framework.

What is a Risk Register?

A Risk Register is a document (or "tool") used as part of the risk management process to record identified risks, mitigating controls and their assessments. A Risk Register would list the identified risks and organise them according to categories (to facilitate their management and the preparation of reporting information). Descriptions of mitigating controls would also be included, in relation to each documented risk, as well as assessments of the risk in terms of Inherent Risk (a product of the 'Likelihood' of each risk occurring and the potential 'Impact' of each risk if it did occur) and Residual Risk (the risk that remains in the business, assessed in the same manner, after the application of the mitigating controls). Risks will originate throughout the business therefore the Risk Register will need to consider risks on an 'enterprise-wide' basis.

The Risk Register would typically be the responsibility of the Compliance Manager and therefore be part of the 'second line of defence' controls operated by the firm.

How does the Risk Register fit within a risk management framework?

The Risk Register is an important component of a Risk Management Framework and would initially be developed as part of a risk identification process, which is the first step in the risk management process. The initial identification of risks within the firm, associated mitigating controls, and the results of the assessment work would be recorded in the Risk Register. The Risk Register would then be updated on an ongoing basis, e.g. recording updated assessments and adding new risks as they are identified.

Once risks have been identified (and recorded in the Risk Register) they would be prioritized for treatment based on their assessment of Inherent Risk. Prioritisation helps firms to focus their efforts, and available resources, on the most significant risks first and to develop appropriate strategies to manage those risks.

The Risk Register would then be used on an ongoing basis as a tool to facilitate the monitoring of risks and the preparation of management reporting information. Updates would typically need to be made to reflect any changes in the identified risks, mitigating controls and their respective assessments that will inevitably take place over time.

Key stages in developing a Risk Register

The typical stages involved in developing a Risk Register are:

1. **Identify risks**: This involves identifying risks that could impact the business. This can be done through brainstorming sessions, interviews with stakeholders, and a review of historical data and past experiences. The majority of risks are likely to come from the first line of defence – the participation of business functions throughout the firm is therefore critical in identifying risks (both initially and on an ongoing basis). Risks should be categorised to facilitate their organisation and management.
2. **Document risks:** The Risk Register is used to document all identified risks (and their assessments – see below) together with the associated mitigating controls. The scope of the Risk Management Framework must be enterprise-wide therefore risks will originate from across the entire business.

   Risks that will be documented in the Risk Register will be those that require management – risks that have been identified and then Avoided or Transferred would not be recorded.

   Risks that have been Accepted, because they are currently assessed as being within the firms' Risk Appetite, should be documented since their assessments may change over time. It is important to regularly review and update the Risk Register as the business develops, in order to ensure that it remains current and accurate.
3. **Assess Inherent Risk**: Once risks have been identified, they need to be assessed in order to determine their 'Likelihood' of occurrence and potential 'Impact'. Likelihood and Impact scores would be allocated and combined to provide an Inherent Risk Score (see below). Inherent Risk is the measure of risk before the application of the mitigating controls.
4. **Prioritize risks:** Risks are typically prioritized based on their Inherent Risk Score in order to help firms focus their efforts on the most significant risks first. As described above, the calculation of an Inherent Risk Score (based on Likelihood and Impact) is a common method. Likelihood and Impact scores could be combined, in accordance with the table below, to provide Inherent Risk Scores of Low / Medium / High / Extreme.

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.

5. **Document mitigating controls:** Risks that have been documented in the Risk Register, and have been assessed and prioritised for treatment, should have associated mitigating controls allocated to them. These may exist already or may need to be developed. A description of the mitigating controls associated with each documented risk would also be included in the Risk Register.
6. **Assess Residual Risk:** The risk that remains following the application of mitigating controls is referred to as Residual Risk. The Residual Risk should be assessed, in a similar manner to the assessment of the Inherent Risk, and documented in the Risk Register. The mitigating controls, if effective, should reduce the Likelihood of the risk occurring, and potentially the Impact.

Risk Register structure

There are many ways to structure a Risk Register and the specific format will depend on the requirements of the firm. However, most Risk Registers will need to include certain descriptions, and information, as described in this guide, in order to provide the user with an understanding of the risk (i.e. a clear and reasonably detailed risk description), the mitigating controls applied to the risk and the assessments of both Inherent Risk and Residual Risk.

The following information should be included as a minimum:

- **Risk reference**: A unique identifier for each risk, such as a risk number or code.
- **Risk description**: A description of the risk, including the potential cause and impact of the risk, sufficient to enable the user to understand the risk (noting that the user of the Risk Register may not be the owner of the risk).
- **Likelihood of occurrence**: An assessment of the Likelihood that the risk will occur, using a numerical score or scale.
- **Impact**: An assessment of the potential Impact of the risk if it does occur, also using a numerical score or scale.
- **Mitigation description**: A description of the mitigating controls that have been applied, or will be developed, to mitigate or manage the risk to acceptable levels (i.e. reduce the Residual Risk to below the Risk Appetite).
- **Risk owner**: The role responsible for monitoring the risk (i.e. updating the description and performing the risk assessments) and implementing the risk mitigation controls. Roles are better documented that individuals given that individuals can change over time.

Risks would typically be grouped in accordance with risk categories and sub-categories in order to facilitate the management of risk and the production of reporting information.

The extract below provides an illustration of a typical Risk Register structure (for a small number of risks).

Last reviewed: [date]
[Company name]

RISK REGISTER *Version [...]*

Reference	Risk category	Inherent risk description	Risk owner	Likelihood	Impact	Inherent Risk score	Current mitigating controls	Residual risk R/A/G	Suggested / planned further action
BUSINESS RISK									
STR001	**STRATEGY**	Strategy is not clearly communicated, understood or reflected in the business plan / financial forecast	CEO	2	3	6 - Medium	Strategy approved at Board level and communicated to the Finance function. Financial forecast is approved by the Board and used to monitor actual performance.	Low	
STR002		Strategy does not address certain markets (geographical or customer) that may become key to the future success of the business	CEO	1	3	3 - Medium	Strategy in place and updated on a periodic basis. The strategy and prioritisation of markets based on management's industry knowledge.	Low	
MAR001	**MARKET**	Dependence on a particular market to drive / maintain growth results in a lack of diversification and increased risk	CEO	2	4	8 - High	Strategic planning at Board level considers potential new markets. Board approval of business cases prepared for new markets.	Medium	
MAR002		Growth in the key markets is slower than expected, adversely affecting servie development	CEO	2	2	4 - Medium	Feedback will be collected through customer questionnaires on quarterly basis and for major customer feedback will be collected through ongoing relationship management.	Low	
PRO001	**PRODUCT**	Issues with the underlying technology affect service performance	CTO	1	4	4 - Medium	New applications / enhancements are defined, monitored and subject to pre-launch testing.	Low	
PRO002		New product development without initial engagement of business functions to determine legal and regulatory implications	CEO	1	4	4 - Medium	Launch of a new product must be approved by the Board and any legal and regulatory concerns addressed before further development. The Compliance Manager will be involved in development activities to ensure that regulatory requirements are met.	Low	
PRO003		Current products/services are unavailable to clients due to regulatory changes.	CEO	1	5	5 - High	Strategic planning at Board level considers potential new markets and products. Board approval of business cases prepared for any new markets.	Low	
OUT001	**OUTSOURCING**	Failure of a key service provider	CEO	1	4	4 - Medium	Due diligence will be performed on service providers before entering into a new business relationship.	Low	
OUT002		Service provider fails to provide services that meet requirements	CEO	1	4	4 - Medium	Contractual agreements are put in place to govern all outsourced services and will specify service description, service levels, complaint routes and termination rights. All outsourced services will be subject to oversight by an appropriate person.	Low	
OUT003		Outsourced services do not support, or conflict with, operational functions	CEO	1	4	4 - Medium		Low	

Note: a template Risk Register has been developed by PACNET that could be used by firms as a starting point for further update. The template includes a significant number of example risks that could be used by to guide firms. The template is significantly detailed, has involved substantial development work, and is therefore available for sale by contacting enquiries@tudorstride.co.uk