Gabriella Lamanda – Zsuzsanna Tamásné Vőneki

Hungry for Risk

A risk appetite framework for operational risks

Summary: The economic crisis, subsequent regulatory changes and the practical lessons learned all indicate that the identification and measurement of risk appetite, as well as its incorporation into strategic planning and risk management will increasingly become a requirement for companies. Our paper seeks to identify ways to comply with this expectation and the potential benefits of compliance. We will explain these through operational risks that affect the entire organisation and are not specific to any sector. In practical implementation, it is essential that, taking into account the specificities of the company and its environment, certain simplifications are made in comparison with the literature. Taking a simpler approach initially and enhancing it according to the lessons learned, in the longer term it is possible to develop an organisation that is more risk aware and is capable of responding to changes flexibly and quickly.

Keywords: risk appetite, risk tolerance, operational risk
JEL code: G21

In the aftermath of the corporate failures and financial scandals of the past decade and a half, and of the events occurring during the financial crisis, authorities have stepped up their requirements for responsible corporate governance and reinforced internal lines of defence. One element of this process is the implementation of enterprise risk management (ERM), a comprehensive risk management system. Citing a number of sources, *Cormican* (2014) aptly captures the essence of ERM as being a value-creating approach which contributes to the definition and development of the appropriate risk strategy through the identification, analysis and continuous monitoring of a wide range of risks. As a result, risk awareness may become an essential corporate value, allowing a company to respond more efficiently to the challenges of its operating environment before any spillover and significant increase in losses. An integral part of ERM is the establishment of a risk appetite framework (RAF). A number of surveys[1] have found that defining this concept is a major challenge for companies, and capturing it even more so. The field has no established and clarified common language, and it is not clear how theoretical approaches may be adapted to a 'flesh and blood' company. This is what our paper attempts to identify, relying on literature and research published on the subject, as well as our own experience, gained primarily in the credit institution sector. Among other things, we seek to determine the criteria against which a viable and useful risk appetite framework may be established. We are also concerned with the principles set out in literature, and how they should and may be interpreted in the course of practical implementation. We are of the view that there

E-mail address: lamanda@finance.bme.hu

is no single tested recipe. It is also relevant to consider what benefits the implementation of RAF can offer for a company.

The process of the establishment of RAF, and associated challenges, is presented through the example of operational risk, which is by its nature not specific to banks. Consequently, our assumptions and findings may also be relevant for operators outside the financial sector.

RISK APPETITE

In an overview of the literature on risk appetite, we find a relatively large number of research papers and analyses focusing on investors' risk preferences.[2] A significantly smaller number of publications are available on the expression of companies' risk appetite. Our paper explores the latter issue.

Risk appetite (also referred to as risk propensity or risk level) shows the types and extent of the risks an organisation is willing to take in order to achieve its strategic goals (COSO, 2012). All of the definitions capturing risk appetite [including BCB (2011); FSB (2013)] focus on strategic goals and the risks that need to be taken to achieve them. The types of risk that may affect a company are determined by its activities, profile, organisational structure, operating environment (competition, legislation, macroeconomic situation, technologies used, etc.), as well as the associated prospects and expectations. A company must take into account all of these in determining its preferences for specific types of risk; which risks need to be taken to ensure that the goals are achieved and the expected return is realised (Towers Watson, 2013b). Following the establishment of risk preference, the level of risk that a company is willing to take needs to be determined. Pursuing this line of argument, the question arises as to how this acceptable level of risk may be determined. To give a considered answer to this question, it is essential to clarify additional concepts related to risk appetite, which provide for a practical understanding of risk appetite itself.

These include the following:

- risk tolerance
- risk limits
- risk capacity.

Risk tolerance is different from risk appetite in that the latter is defined at a strategic level and is determined by senior management (supervisory board), while the former is of an operational and tactical nature and is defined in terms of specific organisational units or projects (COSO, 2012). With regard to the approaches collected by RIMS (2012), risk tolerance (as opposed to appetite) typically involves quantitative approaches that are defined in terms of narrower categories such as risk types, organisational units or specific projects. In other words, it allows actual exposure to be captured, specified and monitored. For example, a range defined relative to the *risk target*, indicating the leeway of the company between the minimum required and maximum acceptable levels of risk exposure.

Risk limits are closely related to tolerance (Goldstein – McElligot, 2014). Their role is to promote an appropriate degree of risk diversification (i.e. to ensure that the risk undertaken is not concentrated on a single counterparty, sector, currency, etc.), and to indicate when and what level of intervention is necessary. With risk appetite, as we wrote earlier, the key concern is the distinction between *acceptable* and *unacceptable* levels of risk. The range between the two represents *tolerable* risk. This is further broken down according to limits, which can be effectively matched with the highly representative classifications of green, amber and red as also used with risk maps (IOR, 2009).

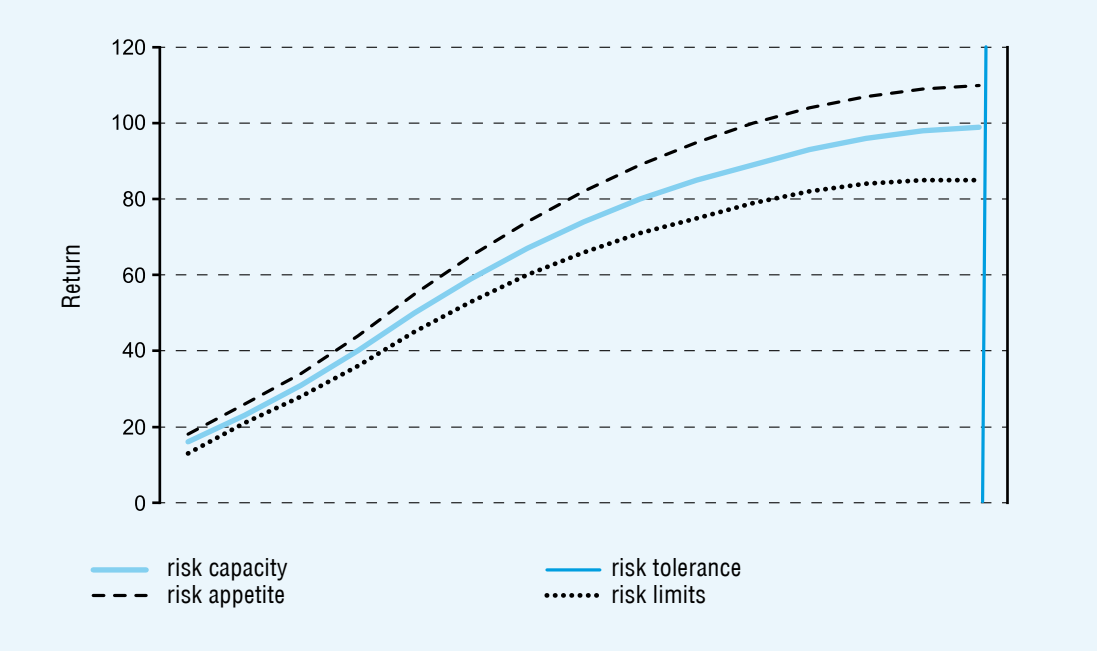
According to *Goldstein – McElligot* (2014), *risk (bearing) capacity* is the maximum risk an institution is still capable of bearing in any given circumstances without any major harm to its equity, liquidity, reputation or regulatory compliance. It is a 'broader' category than risk appetite, since it includes those buffers which protect the company's capital liquidity, etc. when unexpected events occur. Focusing on credit institutions, due to the strict capital adequacy requirements applicable to them, this may also be expressed as the maximum risk that a bank may undertake with a given capital level (available capital), or the extent to which capital may be channelled according to changes expected in the future and whether capital needs to be raised (monitoring of the *maximum risk exposure limit* – MREL). The risk appetite of a company may be higher than its risk capacity. In such cases, resources need to be reengineered, restructured or extended. Using our banking example, a capital increase is warranted. The 2008 crisis offers many examples of cases where companies' risk appetite was excessively high relative to their actual risk capacity. Consequently, the crisis shattered market segments and entire industries. At the same time, it should also be noted that during the crisis, turbulences emerged and developed that market participants failed to consider when determining their risk appetites and exposure. One example is correlations between specific markets, which lead to a loss of confidence on a global scale. That is, the situation was exacerbated not only by excessive risk appetite but also by an inappropriate specification of the degree of risk undertaken.

The relationship and difference between the concepts is illustrated by *Chart 1*.

The problems of definition discussed above also highlight the major challenge in the es-

Chart 1

RISK APPETITE AND RELATED CONCEPTS



Source: Goldstein – McElligot (2014) p. 9

tablishment of a risk appetite framework (RAF): identifying and calculating the risk appetite, as well as channelling it into both risk management activities and the process of strategic planning. Once the company's strategic goals and the associated expected returns are known, each risk category (appetite, tolerance, capacity, etc.) must be assigned an appropriate target. The targets may be set using either a *top-down* approach (e.g. senior management statements on strategy, specification of aggregated exposure, etc.), or a *bottom-up* approach (e.g. product-level limits, sector limits, loss amounts specified by risk type, etc.), or a combination of the two. It is important to monitor the changes in risk exposure and its connection with the specified limits, tolerance levels and risk appetite. Regular monitoring provides feedback that allows the RAF to be further developed as required. Another key criterion is that the RAF is properly communicated within the organisation to ensure that it is integrated into the operations of the company, whereby the benefits of the RAF can be exploited. Potential benefits of RAF include improved strategic planning, better allocation of resources (targeting overexposed areas), improved clarity of decision making, and a better understanding of the interdependencies of connections and objectives, improved commitment, risk awareness, etc. through a specific alignment of operational and strategic objectives. (Marsh and University of Nottingham, 2009)

In summary of the surveys on corporate risk appetite including *Lamanda* (2011), *Towers Watson* (2013a), EY (2013) and BCBS (2014), the general conclusion may be drawn that in most companies, the establishment of RAF is in its early stages, and is predominantly captured by qualitative means and using *top-down* approaches. Challenges are presented by the involvement of lower levels, hence the use of *bottom-up* and quantitative approaches, in the absence of which it is not possible to gain a more detailed picture of specific risks through the involvement of operational units.

The risk appetite framework will be explained in detail in terms of operational risks.

OPERATIONAL RISK

While it is advisable that risk appetite is defined at an institutional level, the scope of this paper does not allow all types of risk to be addressed. Our field of choice is that of *operational risks*, through which we present the methodological approaches for the identification of risk appetite, as well as the opportunities and pitfalls involved in the various approaches. The rationale for our choice is partly that operational risk management is our field of expertise, and partly that this type of risk is relevant to both credit institutions and participants in the non-financial sector.

The definition, management and regulation of operational risk do not have a long history among the participants of the financial sector. Initially, the concept of operational risks was introduced, and the requirements for market participants to measure and manage such risks at a systemic level and to provide coverage through capital imposed by the Basel II risk management and capital allocation framework and the corresponding legislation (in the European Union, the Capital Requirements Directive [CRD]). According to the definition provided by the Basel Committee on Banking Supervision (BCBS) which developed the Basel II Capital Accord, operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems failures or external events. In order to promote practical applicability, the Basel Committee

breaks down operational risks into 7 event types and bank operations into 8 business lines. The event types are: internal fraud, external fraud, employment practices and workplace safety, improper business practices, damage to tangible assets, business disruption and system failures; and improper process management [for more details, *see Table 1* and Lamanda – Zsolnai (2010)].

In many respects, operational risks are different from those conventionally considered bank risks (market and credit risk); moreover, as practising professionals, we argue that their management does not require different approaches and methodologies for companies operating in the financial and the non-financial sectors. As opposed to market and credit risk, operational risk [based on IOR (2009), Lamanda (2011) and Homolya (2012)]:

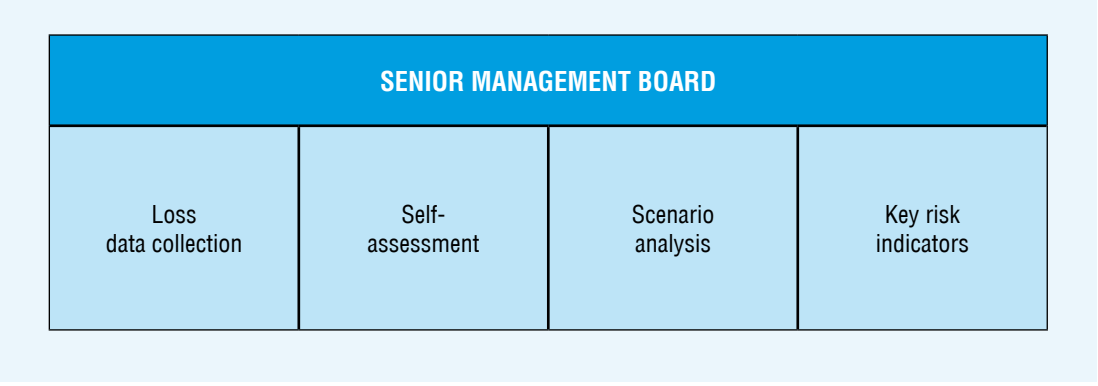
- appears in every organisation regardless of its sector, as both financial and non-financial institutions face the consequences of natural disasters, human error, legislative changes, hacker attacks, etc.;
- is a heterogeneous type of risk that is difficult to define; as shown by the diversity of event types, the number of potential events may be extremely high. As practising professionals, we add newly emerging events to the list of potential operational risks on a regular basis;
- exposure is difficult to define, as the range of risks becomes wider and changes continuously;
- the risk/return correlation is not applicable for operational risks. Additional risk is not undertaken to achieve additional return. Operational risks must be faced in any case. Instead of the risk/return correlation, the risk/cost correlation applies, i.e. the cost implications of risk-mitigation measures taken must be compared to potential loss;
- this covers both frequent and low-impact events (cash deficit, loss of documents, damage to vehicles) and rare but high-impact events (earthquake, disruptions to core systems lasting several days, war);
- poor measurement reliability due to lack of relevant data and experience (backtesting). Operational risk models have only existed for a few years and the requirements for such models have yet to be standardised. The lack of historical data makes risk measurement even more difficult;
- risk management requires the participation and commitment of the entire organisation. The heterogeneous and diverse risks can only be identified and monitored through the establishment of a well-designed and trained internal network. Without such a network, a central risk management organisation comprising a few staff will not be functional. To manage operational risk, a framework covering and mobilising the entire organisation must be established and integrated into corporate culture.

In choosing the tools to measure risk appetite, the sources of information available on the operational risks occurring in the company concerned need to be examined. Essentially, four pillars may be identified which can provide the information to be collected on risks for the parties involved in the risk management process *(see Chart 2).*

The top of the chart shows the senior management board which both supervises and supports the operational risk management system. Practical experience shows that support and commitment from senior management and the involvement of the entire organisation require the operation of a formal committee (Operational Risk Committee), regular sessions and an extension of members' responsibilities in connection with the discharge of the supervisory functions of the operational risk system and the making of decisions concerning risk management.

Chart 2

OPERATIONAL RISK MANAGEMENT FRAMEWORK



Source: Author's own editing

The first and most robust data source for operational risk management is the collection of loss data for the purpose of understanding the past. Data collection involves efforts to compile a database on materialised risks and the losses incurred or gains realised, which is the widest possible in scope, but is standardised in terms of structure and is suitable for statistical analysis, to serve as a starting point both for capital calculations and measures to mitigate risk.

Information from external loss databases may help to resolve the problem resulting from the short time series available on losses and from the absence of experience, and to outline extreme scenarios.

The second pillar is the practice of *risk and control self-assessment* (RCSA), which takes the form of interviews, workshops and brainstorming and is intended to explore the future. Self-assessment seeks to identify the operational risks which must be faced in the period ahead (usually, in the next financial year), the probability of their occurrence, and in the event of their occurrence, their impact on the operations and profitability of the organisation. Self-assessment also involves an assessment of the control environment, as part of which an examination is carried out to determine whether the system's in-built controls supporting the identification of risks exist, and the efficiency of their operation.

The third source of information on operational risk is the practice of scenario analysis, which involves the evaluation and analysis of significant risks capable of exerting a 'catastrophic' impact on the operations of the organisation. Scenario type risks include, for example, natural disasters, wars, massive loss of employees, longer disruptions to the IT systems supporting critical processes, or in the case of banks, the dreaded bank run.[3]

Key risk indicators (KRIs) are established to enable the deterioration of risk factors to be monitored regularly and any increase expected in loss events to be forecast in periods between self-assessments and scenario analyses, which are usually carried out on an annual basis. To this end we seek indicators which are related to risks such as fluctuation, load indicators, complaints, specific macroeconomic indicators, etc.

In the cases of banks, in addition to the four information packages of differing character explained above, regulatory capital requirement itself may also be considered an indicator suitable for capturing risk appetite, provided that capital requirement is calculated using the Advanced Measurement

Approach (AMA). In such a case, regulatory capital requirement will include the four sources of information in one way or another, complemented by external loss data.

THE OPERATIONAL RISK APPETITE (ORA) FRAMEWORK AND ITS CHALLENGES

Before addressing the various ways of identifying operational risk appetite (ORA), it is appropriate to highlight the fact that in the case of this risk, risk appetite needs to be understood differently than other types of risk. As indicated earlier, an organisation does not take operational risks deliberately, but will unintentionally face such risks by employing people, maintaining buildings, and operating processes and systems in the given political, economic and geographical environment.

Homolya (2007) writes that "[i]n the case of operational risks, risk appetite is not applicable ...", and according to *Shiels* (2011), firms will have no appetite for most operational risks (such as fraud or natural disasters) for moral reasons, and will only tolerate them at some level. On the other hand, the difference between risk appetite and tolerance shown in Chart 1 results from the associated levels of gains, which is not applicable in the case of operational risks. Arguably, therefore, in the case of operational risks, appetite and tolerance are not distinguished. While in terms of the terminology, 'tolerance' is preferred in literature and by some professionals, in view of the fact that appetite is obviously applicable to other types of risk (credit and market), we will use 'operational risk appetite' (ORA) to help establish a common language and to provide the possibility of mutual integration.

In defining operational risk appetite, we seek to determine what should and can be adopted from literature in order to obtain a framework that is both clear and useful.

In terms of the concepts outlined earlier in this paper, risk preference results from the 7 event types, whereas risk limits are thresholds specified for the loss amounts associated with each event type or for KRIs, and the magnitude of risk capacity is represented by the capital allocated to operational risk. Operational risk appetite is best captured as the maximum exposure a company is willing to undertake and tolerate in the normal course of business in respect of each event type.

The ORA framework includes the identification of operational risk appetite, its measurement, monitoring, communication within the organisation, and regular reporting to senior management.

Based on IOR (2009), the appropriate tools for the expression of risk appetite may be selected by following a combination of various approaches. Accordingly, we can rely on *top-down* and *bottom-up* methods, using both qualitative and quantitative approaches. Below we explain the specific approaches are explained in this order.

In the case of *top-down* approaches, it is the senior management (in practice, the *Board*, the *Management Committee,* the *Operational Risk Management Committee*, or their equivalent) which determines the level of the organisation's tolerance for significant risk. This could be a qualitative requirement or a quantified limit. Examples of the latter include (Cyriac, 2009):

- risk appetite defined as a percentage of capital allocated to operational risks, available primarily to credit institutions using AMA;
- risk appetite is identified as the expected value indicated by the operational risk model, and its 'utilisation' is monitored on a continuous basis;
- identification and measurement through the loss amounts associated with various levels of expected revenue growth;

- identification of expected and unexpected losses as a percentage of profits before taxes.

In *bottom-up* approaches, limits are specified, subject to the approval of lower levels of management, for defined risk categories (such as event types or business lines) based on the data collected as part of the operational risk management process, the aggregation of which will produce the value of risk appetite. In following this approach, reliance can be made on loss data reflecting the past, data collected in self-assessment workshops indicating future expectations, and key risk indicators. In respect of loss data, based on their time series analysis, maximum values may be specified for each business line and event type. Self-assessment (RCSA) enables an examination of inherent risk and residual risk as reduced by controls. The application of various indicators (KRI, KPI, KCI)[4] may play a role in the breakdown of risk appetite from a strategic level as well as in its monitoring (Thirlwell, 2013). Scenario analysis, being the fourth source of information, also needs to be discussed. The issue is not frequently addressed in literature, which may be due to the fact that scenario-level events are highlighted and are subject to special examination by virtue of their very magnitude and potentially 'catastrophic' impact, and as such they are not considered as a part of risk appetite to be undertaken. Since the possibility of such events occurring cannot be ignored, they may be included in the qualitative definitions of risk appetite as undesirable events. While establishing ORA, in some cases digressions must be made to the areas of credit and market risks, which are related to operational risks. However, this will not pose any problems if risks are not addressed in isolation and consideration is given to their mutual effects.

Literature mostly considers *top-down* approaches to be appropriate, primarily by virtue of the statements on senior management support and commitment. Top-down approaches can be used effectively and even independently, but primarily in identifying the qualitative components of the risk appetite framework. Indeed, it is essentially such qualitative principles that form the backbone of a company's risk culture (IOR, 2009). The greatest challenge of a *top-down* approach lies in the appropriate breakdown of high-level goals and the measurement of achievement. For that reason, rather than being followed separately, the two types of approach (*top-down* and *bottom-up*) should be taken in combination, to validate each other, as it were. Practical experience shows that information on operational risks, which are heterogeneous and difficult to measure, is available 'at the marches' from the sources outlined in the previous section; consequently, at least in the interests of providing a fair view of the situation and preparing the decisions of senior management, a *bottom-up* approach should be taken first for the identification of ORA.

A qualitative approach links risk to strategic goals, and breaks down strategy to the level of business units through risks. It formulates principles concerning the risks that are considered to be acceptable and unacceptable by an organisation. (E.g. "The bank shall not finance clients whose activities are presumed to be in violation of public morals and social values, or associated with crimes." There are certain elements of operational risks, such as reputational risks and *compliance*-type risks, which can only be captured at the qualitative level. When taking a quantitative approach, risk appetite is expressed in terms of specific figures. Of the types of operational risk information explained earlier, risk appetite may be expressed as a percentage of regulatory capital requirement or as specific loss amounts.

The identification of risk appetite can be detailed further by addressing its time horizon and identifying short-and long-term risk appetite (IOR, 2009).

Based on the foregoing, *Table 1* provides a summary of the methodology and the specific measures against which each approach may be applied in practice to each event type within the rather heterogeneous set of operational risks.

The dimensions of the table suggest that with rationality in mind, the potential forms of expression and approaches must be streamlined. Such a selection must be made by taking two aspects into account. One is what to consider a priority or a dominant risk within each event type (e.g. which risk types result in the highest losses, or which risks are expected to grow in light of the risk trend), and what it is that best captures each risk. The other is the highly practical question of what the company has regularly produced information of adequate quality on in order to apply measures of the required sensitivity appropriately supported by data, and to reduce the cost of their production. Arguably, then, a prominent role in the expression of operational risk appetite may be played by loss data and KRIs. We have already referred to the problems associated with scenario analysis, while in the case of self-assessments, limitations may be imposed by their high degree of subjectivity. As such, self-assessments may provide useful input for the qualitative components of risk appetite. The 'fault' of loss data is that by using them, the appetite for the next period is supported by historical data. This shortcoming may be eliminated by KRIs. In other words, these may be useful tools in combination. It should be noted, however, that in order to leverage this utility, it is essential that KRI thresholds are set so that they reflect the direction and extent of changes in exposure in an objective and timely (preferably predictive) manner, and in adequate quality.

As loss data play an important role in both operational risk management and the determination of the relevant capital requirement, one possible solution is to identify the maximum extent of loss that the organisation can tolerate or undertake both for each event type (possibly further broken down by business lines or groups of business lines) and in aggregate. For this purpose, we can use the red, amber and green categories referred to above. In another approach, in respect of specific categories, the ORA framework is based on qualitative senior management statements, to which quantitative measures are mapped from lower levels of the organisation. This latter may mean the involvement of KRIs or possibly other relevant factors in addition to loss data, to which weights can be applied to obtain composite indicators. In respect of the type 'Clients, products and business practices', the most important objective and statement of senior management may be that "the organisation refuses to take *compliance*-type risks and shall use its best endeavours to ensure that all of its employees work in the strictest compliance with legal regulations and internal policies." The question arises as to how to capture this statement. Partly in terms of relying on loss data such as fines, litigation costs, etc., and partly in terms of KRIs such as the number of complaints and pending court proceedings, and the time required to investigate complaints. Mapping the appropriate limits and thresholds to these enables the adequate monitoring of risk exposure against the bank's risk appetite.

An examination of qualitative and quantitative approaches suggests that both have a specific role to play. Operational risks comprise an extremely heterogeneous group, and some are risk factors that have a considerable history and database (typically

Table 1

OPERATIONAL RISK AND THE ORA FRAMEWORK

Event type	Examples	Measurement options
Internal fraud	misappropriation, unauthorised activity	Top-down: qualitative management principles (e.g. covering circumventions of the law or internal policies)
		Bottom-up: based on risk management process, e.g. number and value of losses, expected and unexpected risks identified as part of self-assessment
External fraud	hacker attack, use of forged documents for credit applications	Top-down: qualitative management principles (e.g. concerning a high level of IT security)
		Bottom-up: based on risk management process, e.g. number, value or ratio (e.g. to revenue) of loss amounts associated with fraud incidents and attempts; expected and unexpected risks identified as part of self-assessment; key risk indicators (e.g. fraud incidents per product, number of disbursements prevented by the fraud system)
Employment practices and workplace safety	harassment, discrimination, loss of key employees, massive loss of employees	Top-down: qualitative management principles (e.g. concerning negative discrimination, employment of persons with disabilities)
		Bottom-up: based on risk management process, e.g. number and value of losses, key risk indicators (e.g. fluctuation, number of labour-related court cases, number of training days), other sources: based on the results of workplace satisfaction surveys and of annual fire safety and work safety assessments"
Clients, products and business practices	unintentional damage to clients, failures resulting from the nature or design of products	Top-down: qualitative management principles (e.g. concerning money laundering or ethical violations)
		Bottom-up: based on risk management process, e.g. number and value of losses (fines and compliance-type losses), key risk indicators (e.g. number of complaints, time required to investigate complaints)
Damage to tangible assets	vandalism, terrorism, natural or industrial disasters, as a result of which the bank's fixed assets or human life is partially or fully damaged, or respectively, assets lose their value	Top-down: qualitative management principles (e.g. concerning incidents threatening human life)
		Bottom-up: based on risk management process, e.g. number or value of losses, risks identified as part of self-assessment, other sources: insurance statistics or business continuity plans (BCP) and disaster recovery plans (DRP)

Event type	Examples	Measurement options
Business disruption and system failures	malfunctioning IT and telecommunication systems and infrastructure	Top-down: specification of critical processes and systems
		Bottom-up: number and value of losses, key risk indicators (e.g. system slowdowns and downtimes for critical systems, outages due to disruptions to external providers), other sources: BCP, DRP and contracts with external service providers
Execution, delivery and process management	reporting failure, misreporting, losses resulting from the loss of documents	Top-down: qualitative management principles (e.g. concerning the number of high-risk findings by internal or external auditors)
		Bottom-up: based on risk management process, e.g. number and value of losses (fines), key risk indicators (e.g. operating costs), other sources: complaints management, recommendations of internal audits and their implementation

Source: Author's own editing

insurable risks), which makes them suitable for the quantitative identification of their acceptable level for the organisation. Such risks include for example natural disasters where appropriate insurance cover enables the accurate amount of residual exposure to be determined. On the other hand, the organisation is helpless with certain risks, the mitigation and management of which depends on factors outside of its control. A solution to the tolerance of such risks may also be provided by qualitative statements.

The measurement of risk appetite is not a one-off task. Where the organisation opts for the implementation of ORA, this will provide it with a new strategic tool, which will result in a change in attitude and will require continuous 'maintenance' and monitoring. Communication, including adjustments based on backtesting, is an integral part of the framework to ensure that ORA serves the strategic goals of the organisation effectively.

Due to its complexity, the conceptual framework established in literature is difficult to adapt to practice. Therefore, as an initial version, it is recommended that a simplified approach is implemented using the available frameworks, data and systems. However, a well-functioning RAF is based on the accurate specification and definition of its components. A common language and the consistent use of terminology will ensure that the approach, which requires the involvement of the entire organisation and senior management support, effectively becomes a useful tool for the implementation of strategic goals. As we have seen, this is a major challenge in the case of operational risks due to the limited availability or absence of data and experience. However, we expect regulatory and supervisory requirements for financial institutions to increase and become stricter in the foreseeable future in connection with the expression of risk appetite. In preparation for compliance with regulatory requirements, it is recommended to start the implementation of the methodologies, the benefits of which may be exploited and are felt in the long term anyway.

Our personal experience is that in many cases, the risk appetite framework is established with support from senior management. Resistance occurs when channelling the RAF into strategic decision making requires the reengineering of existing systems (banking infrastructure), i.e. when there are significant cost implications. As the latter (additional IT-side tasks, process engineering issues and related, potentially significant costs) are indeed characteristic of practice, maximum management commitment to the full implementation of the system may be obtained by highlighting the benefits of RAF, which will manifest both in support for strategic decision making and in improved risk management practice.

CONCLUSIONS

In this paper we provided a summary and a detailed discussion of the principles and components of the risk appetite framework with a view to better understanding and more efficient practical application. We sought to illustrate the process of practical application and the associated challenges from the financial institutions' perspective, but through operational risk, a type of risk that is not specific to banks. We intended to carry out a critical analysis of the available solutions offered in literature so that they can be captured from a practical point of view and can be implemented better.

Literature offers a number of alternatives for the identification of risk appetite, of which the one must be selected that can be adapted to the organisation concerned with its specificities in mind. The robustness of the risk appetite framework, the amount of work put into the establishment of the system, and the form and extent of senior management involvement must be aligned by every organisation to its size, its profile, the level of risk in its operating environment and the information base available to it. It is essential that the company gives priority to simplicity and constructs its risk appetite framework based on standardised, understandable, measurable and presentable factors. Depending on subsequent experience, the RAF may be developed and improved as required.

The establishment of a risk appetite framework prompts the organisation to rethink its activities and processes, which will improve its risk awareness and risk culture, as well as its ability to respond to the challenges of its operating environment better and faster.

In our paper we focused on the difficulties involved in the implementation of risk frameworks and more specifically the ORA. Live application, efficient monitoring and the evaluation of developments present further challenges and as such, further opportunities for research.

Notes

[1] Based on material from the Big Four and also BCBS (2014) and FSB (2013)

[2] See, *inter alia*, Fung, L. K. – Tam, C. – Yu, I. (2009): Changes in investors' risk appetite – an assessment of financial integration and interdependence. IFC Bulletin No. 31. pp. 294–322 www.bis.org; Berlinger, E. – Váradi, K. (2015): Risk Appetite. Public Finance Quarterly 2015/1, pp. 49–62

[3] At first glance, a bank run may be seen as a liquidity risk; however, it requires much more work and preparation in terms of operational risks. In the event of a bank run, capacity problems need to be resolved at branches, on e-channels and in call

centers, and efforts are required to address security issues, external and internal communication, and the supply of foreign exchange and cash.

[4] KRI: Key Risk Indicator; KPI: Key Performance Indicator; KCI: Key Control Indicator.

Literature

Cyriac, J. (2009): Operational Risk Appetite – Why, What & How. 2008–2009. Source: www.slideshare.net/ComplianceTrack/operational-risk-appetite-ora-why-what-how

Cormican, K. (2014): Integrated Enterprise Risk Management From Process to Best Practices. *Modern Economy*. Vol. 5. pp. 401–413

Goldstein, R. – McElligot, J. (2014): Risk Appetite. A Discussion Paper. Central Bank of Ireland http://www.centralbank.ie/regulation/poldocs/dispapers/Documents/Risk%20Appetite%20Paper.pdf

Homolya, D. (2007): Kockázati tolerancia koncepciója és a működési kockázatok területén való alkalmazhatósága (The concept of risk tolerance and its applicability to operational risks). XXVIII. Országos Tudományos Diákköri Konferencia (National Scientific Students' Associations Conference), Doctorandus Conference, Miskolc April 2007.

Homolya, D. (2012): Banki működési kockázat és intézményméret (Operational risk of banks and firm size). PhD Thesis, Corvinus University of Budapest

Lamanda, G. – Zsolnai, A. (2010): Mozgó célpont – a tőkemegfelelési direktíva első pillére (A moving target – the first pillar of the capital requirements directive). Public Finance Quarterly, 2010/1. pp. 154–167

Lamanda, G. (2011): Banki működési kockázatok kezelésének szabályozása és gyakorlata (Regulation and practice of managing the banks' operational risks). PhD Thesis, Budapest University of Technology and Economics

Shiels, A. (2011): Developing an Operational Risk Appetite: Turning a "black art" into practical reality. January 2011. (Avantage Reply) http://www.frm.reply.eu/

Towers Watson (2013a): Risk and Finance Management Survey 2013. http://www.towerswatson.com/en/Insights/IC-Types/Survey-Research-Results/2013/04/2013-Risk-and-Finance-Manager-Survey

Towers Watson (2013b): Another bite at the apple. Risk appetite revisited. 2013. https://www.towerswatson.com/DownloadMedia.aspx?media=%7BFF9D7227-D316-45E0-8E42-6C1E51716CAA%7D

Basel Committee on Banking Supervision, BCBS (2011): Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches. http://www.bis.org/publ/bcbs196.pdf

Basel Committee on Banking Supervision, BCBS (2014): Review of the Principles for the Sound Management of Operational Risk. 6 October 2014. www.bis.org/publ/bcbs292.htm

Committee of Sponsoring Organizations, COSO (2012): Enterprise Risk Management – Understanding and Communicating Risk Appetite. http://www.coso.org/documents/ERM-Understanding%20%20Communicating%20Risk%20Appetite-WEB_FINAL_r9.pdf

Ernst&Young, EY (2013): Remaking financial services: risk management five years after the crisis. A survey of major financial institutions.

http://www.ey.com/Publication/vwLUAssets/Remaking_financial_services_-_risk_management_five_years_after_the_crisis_-_Complete/$FILE/EY-Remaking_financial_services_risk_management_five_years_after_the_crisis.pdf

Financial Stability Board, FSB (2013): Principles for an Effective Risk Appetite Framework. http://www.financialstabilityboard.org/wp-content/uploads/r_130717.pdf?page_moved=1

Institute of Operational Risk, IOR (2009): Operational Risk Sound Practice Guidance. Risk Appetite. December 2009. www.ior-institute.org

Marsh and University of Nottingham (2009): Research into the Definition and Application of the Concept of Risk Appetite.

The Risk Management Society, RIMS (2012): Exploring Risk Appetite and Risk Tolerance. Executive Summary. www.rims.org.