Systematic Approach to Operational Risk Management in Central Banks (Regulators): Prerequisites, Current Issues, and Development Prospects

Valery Goreglyad, Bank of Russia

As regards financial risk management, its issues have already been worked through rather extensively both in theory and in practice. However, this is not the case when it comes to operational risks. The reason for this does not lie in the two types of risk having differing levels of significance (both types can have disastrous consequences for an organisation); it is rather due to their differing nature and, in the case of operational risks, more complex cause and effect relationships between the sources and consequences of risks. These circumstances make it extremely challenging not only to assess, but also to understand operational risks. Moreover, whereas a lot has already been done in regards to the operational risks faced by commercial institutions (which is largely thanks to the efforts of supervisory bodies who consider this a matter of financial stability), it is only in the last two decades that supervisory bodies themselves (central banks and other regulators, hereinafter referred to as regulators) have been seen to implement operational risk management systems. In this paper, we analyse the prerequisites for the formation of a systematic approach to operational risk management in international practices and conduct comparative analysis of its reasonableness for using by regulators and commercial institutions. Our analysis confirms the relevance of this new trend and demonstrates that, given their specific nature, when regulators implement operational risk management systems in their activities, risk culture and top-down support issues come to the fore.

Keywords: central banks, risk management, operational risk

JEL Codes: G30, E58

Citation: Goreglyad, V. (2019). Systematic Approach to Operational Risk Management in Central Banks (Regulators): Prerequisites, Current Issues, and Development Prospects. Russian Journal of Money and Finance, 78(4), pp. 99–118. doi: 10.31477/rjmf.201904.99

1. Introduction

Regulators have leaned towards implementing a systematic approach to operational risk management since the late 1990s. This approach presupposes
that an organisation employs uniform rules for identifying and assessing risks, that the results of these procedures are embedded in the decision-making process, and that a subdivision will be created to coordinate the relevant work.

Figure 1 shows that 47 regulators created a centralised unit for the coordination of operational risk management in the last 24 years (from 1996 to 2019), with the majority of them (39) introducing it from 2001 to 2015.

The implementation by regulators of a centralised operational risk management methodology was accompanied by the creation of global forums for the exchange of professional expertise and opinions in this sphere.

The International Operational Risk Working Group (IORWG) created in 2005 by the Bank of Spain and the Federal Reserve Bank of Philadelphia and uniting 17 regulators can be considered a key platform of this kind. In 2016, the Bank of Russia also became a member of IORWG and the bank’s directors set the task to implement a systematic approach to operational risk management. Currently, the number of IORWG members has reached 101; they include regulators from 96 countries worldwide (some countries are represented by two regulatory bodies) and a number of supranational organisations such as the International Monetary Fund (IMF), the Bank for International Settlements (BIS) and the European Central Bank (ECB).

The last two decades have seen international organisations paying close attention to the operational risk management undertaken by regulators. In particular, the Bank for International Settlements conducted a study (2009) devoted to how regulators organise operational risk management. The IMF assesses the organisation of risk management as one of the key criteria of regulators quality in the countries that are potential borrowers from the Fund. The assessment takes into account their risk profiles, risk culture, and resources available.¹

In his review of operational risk management practices in regulators, Khan (2016) concludes that they do not pay sufficient attention to this issue and gives recommendations on how to fully integrate an operational risk management system into all areas of a regulator’s activities. However, those practices were originally developed for commercial organisations, not regulatory institutions. Hence it should be asked if the practices are relevant for the fundamentally different

¹ The staff numbers in specialised subdivisions coordinating this work accounts for more than 1% of the total number of staff in 60% of regulators that employ uniform approaches to operational risk management.
nature of the latter. This issue has not been comprehensively covered in either economic literature or in studies undertaken by reputable organisations.

The analysis conducted in this paper shows that the specifics of regulators’ activities are the main reason why it is so difficult to implement a systematic approach to operational risk management into regulators’ operations. While commercial institutions are incentivised by financial viability (or requirements set by regulators), it is not so obvious to a regulator’s staff why it is necessary to implement these practices into their daily work. As a result, it is only possible with two conditions. First, the support of top managers understanding the value of this system for the organisation as a whole. Second, the availability of qualified specialists from the risk management subdivision able to properly implement the system taking into account all the specifics of the regulator’s activities.

The aim of this paper is to identify the factors substantiating the need for and particular features of such systems in regulators’ activities, as well as to determine the main problems in this field.

This paper is structured as follows. Section 2 contains analysis of the prerequisites for the formation of a systematic approach to operational risk management, reveals its potential in commercial organisations and explains the need for its use by regulators. Section 3 focuses on analysis of the ‘settings’ of an operational risk management system necessary for regulators taking into account their specifics, as well as the study of related problems. Section 4 provides the analysis of the trends and prospects for further development in this field. Findings are summarised in Section 5.

2. Prerequisites for the implementation of a systematic approach to operational risk management by regulators

Analysis of regulators’ practice of introducing a systematic approach to operational risk management, which, as noted above, started in earnest in the 1990s, shows that the reasons behind this phenomenon are far from being theoretical.

Risk theory as an independent scientific field, as a comprehensive system of concepts and approaches, has yet to be developed. It gives only a general idea of the risks, their nature and the methods used to manage them without reference to specific conditions of the internal and external environment and the necessary ‘system settings’.

The most famous risk studies have been mainly of a specialised nature, through the lens of other scientific schools (mathematics, physics, economics, cybernetics, etc.). In particular, risk management issues were first studied within the scope of probability theory by well-known mathematicians and physicists, such as Christiaan Huygens, Jacob Bernoulli, Blaise Pascal, and Pierre de Fermat. Moreover, these studies generally stemmed from specific practical needs.²

² E.g. as is known, the development of probability theory was largely driven by the search for scientifically proven ways to win at gambling.
Therefore, one cannot but agree with the economists and experts who argue that risk management in any given organisation, and in particular operational risk management, is a practical discipline, rather than a science. Thus, the issue of risk management, which includes the development of a systematic approach to risk management, requires knowledge with regard to the specifics of the internal and external environment associated with the functional objectives of a particular organisation.

Therefore, in order to identify the prerequisites for regulators introducing a systematic approach to operational risk management, we will analyse practical issues. This analysis shows that it would be incorrect to examine this trend in isolation from the events that occurred in the global economy, and, above all, from the events in the commercial sector.

2.1. Dynamic development of risk management and creation of a systematic approach to operational risk management since the 1990s

Using the risk-management terminology, the root cause why risk management issues became so urgent during the period in question was that the society once again realised that market mechanisms were far from being perfect.

Several decades of economic growth had led to economic institutions paying less attention to the control environment, and profit maximisation became a priority. Individuals and enterprises often received loans despite obvious signs of their low creditworthiness, and clearly risky investments were made. It was increasingly convenient to view the control environment as an outdated concept that was no longer compatible with market realities and hindered profit making. This trend was further compounded by insufficient attention from the government.

A series of crises in the late 20th – early 21st centuries, bankruptcies of major corporations, and unprecedented financial frauds, including the cases involving Polly Peck, Bank of Credit and Commerce International, Maxwell Communications, Enron, WorldCom, Lehman Brothers, Merrill Lynch, AIG and others, revealed the fallacy of relying on market self-regulation and dispelled the myth of governments automatically stepping in to save too big to fail organisations.

When analysing the causes of financial shocks, both business and the government focused on the quality of management. This analysis was the springboard for the dynamic development of the concept of internal control, and then the broader topic of risk management.

One of the most famous works, which publication heralded the onset of intensive studies of the topic, is what is referred to as the Cadbury Report.

---

3 Control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organisation (COSO, 2013).
(Committee on the Financial Aspects of Corporate Governance, 1992). This is a report issued by a committee specially created in 1991 that included representatives of both the government and business in the United Kingdom.

The report was compiled following the bankruptcies of key companies, which ‘... had raised concerns about the working of the corporate governance system.’ Its authors emphasise the key role of the board of directors in managing the company and highlight the need to strengthen its control functions, as well as the role of auditors. The Cadbury Report’s main recommendation is that all companies registered in the United Kingdom are obliged to confirm their adherence to Code of Best Practice when listing on the London Stock Exchange.

The report contains a key tenet regarding the role of internal control in corporate governance: ‘Since an effective internal control system is a key aspect of the efficient management of a company, we recommend that the directors should make a statement in the report and accounts on the effectiveness of their system of internal control and that the auditors should report thereon.’

Another in-depth study of internal control issues during that period was also conducted as part of the study carried out by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) established in 1985. COSO’s recommendations on internal controls, Internal Control – Integrated Framework (Committee of Sponsoring Organizations of the Treadway Commission, 1992), formed the basis for a number of corporate governance systems.

Following the Cadbury Report, a series of other well-known reports that elaborated the topic of corporate governance (see Table 1) were published. They included the Turnbull Report (Institute of Chartered Accountants in England and Wales, 1999), which is one of the first studies that underscores the necessity of internal control focus on risks and the board of directors’ responsibility for the effective management of risks.

| Report (study) | Year | Main topic |
|---------------|------|------------|
| Greenbury Report (Study Group on Directors’ Remuneration, 1995) | 1995 | Renumeration of directors |
| Hampel Report (Committee on Corporate Governance, 1998) | 1998 | Review of the Code of Best Corporate Governance Practices given in the Cadbury Report (Committee on the Financial Aspects of Corporate Governance, 1992) |
| Turnbull Report (Institute of Chartered Accountants in England and Wales, 1999) | 1999 | Directors’ responsibility for the operation of the internal control system and the presence of an audit that ensure high-quality reporting and fraud prevention |
| Myners Report (Myners, 2001) | 2001 | The role of institutional investors |
| Higgs Report (Higgs, 2003) | 2003 | The role of non-executive directors |

The Turnbull Report emphasises that ‘the board of directors must take into account risks, risk appetite, the ability to control risks and the economic viability
of control procedures in terms of costs and benefits of their implementation. The system of controls should be comprehensive and include procedures that make it possible to inform about losses and deficiencies, as well as measures taken should they occur.’

At the turn of the 1990s–2000s, a number of similar studies were conducted, and reports, recommendations and legislative initiatives were prepared with the aim of tightening and expanding corporate governance requirements. They include the Core Principles for Effective Banking Supervision, prepared by the Basel Committee on Banking Supervision (1997), the OECD Principles of Corporate Governance, published by the Organisation for Economic Cooperation and Development (1999), and the Sarbanes-Oxley Act (107th United States Congress, 2002) adopted by the US government.

As a result, internal control and then risk management as a more fundamental category started to evolve as the logical continuation of the development of corporate governance in general. Subsequently, this formed the basis for the ‘three lines of defence’ concept (Committee of Sponsoring Organizations of the Treadway Commission, 2015).

It is important to understand this development in order to effectively organise risk management. Only by understanding that it is a part of corporate governance that must be ‘fully integrated’ and bound with other parts, an organisation as a whole will be able to function as efficiently as possible.

A further quality loop in the development of risk management took place in 2002–2009 when the banking community started to make the transfer to Basel II (2004), which had a primary goal of improving the quality of risk management in banking institutions. A number of standards and practical guidelines were also published that together created a ‘coordinate system’ for the modern operational risk management system. The key (most complex) examples are the COSO Enterprise Risk Management – Integrated Framework (Committee of Sponsoring Organizations of the Treadway Commission, 2004) and the HM Treasury Orange Book: Management of Risk Principles and Concepts (HM Treasury, 2004).

This period is characterised by risk management being finally accepted as part of corporate governance that includes an internal control system. Internal control was integrated into risk management. As it was said in the aforementioned COSO paper, the new standpoint provides ‘a more robust and extensive focus on the broader subject of enterprise risk management. It is not intended to and does not replace the internal control framework, but rather incorporates the internal control framework within it.’

Subsequent financial shocks, primarily the 2008 crisis, inevitably influenced the global community’s views on risk management. Key events include the introduction of Basel III, the revision by the Basel Committee on Banking Supervision of the Core Principles of Effective Banking Supervision, the establishment of the Financial Stability Board, the revision of the standards of
the Financial Action Task Force, and the tightening of supervision. But these were rather fine, albeit significant, tuning of established risk management systems.

Let us briefly look at the elements forming an operational risk management system and its potential.

### 2.2. Systematic approach to operational risk management

This paper is not aimed at encompassing all the elements of an operational risk management system and their interrelatedness. We will briefly look at the key elements that are vital to the effective functioning of the entire system and their benefits.

#### Table 2. Key elements of an operational risk management system

| No. | Element                                                                 | Aim                                                                 |
|-----|-------------------------------------------------------------------------|---------------------------------------------------------------------|
| 1   | Uniform coordinate system (including terminology, goals, objectives, principles) | Ensuring a uniform understanding of the same risk management issues by all employees |
| 2   | Organisational structure of the risk management system                  | Ensuring transparency and, as a result, a better understanding of the powers and responsibility for risk management |
| 3   | Risk management processes (identification, assessment, response, monitoring and reporting) | Ensuring consistent and continuous identification of and subsequent work with risks |
| 4   | Risk management procedures (registering events, self-assessment, etc.)   | Ensuring the effective implementation of risk management processes in practice |
| 5   | Completing risk management procedures by decision-making               | Ensuring integration of risk management (risks are fully considered) into decision-making processes |
| 6   | Identification of significant risks by setting the criteria of significance | Focus only on significant risks that may materialise and entail noticeable consequences |
| 7   | Allocation of significant risks to their owners                         | Increased responsibility for specific negative events (risks)         |
| 8   | Unified registers and risk assessment scales                            | Ensuring comparability and making it possible to subsequently rank risks |
| 9   | Risk ranking tools (including heat maps)                               | Increased capability for risk prioritisation with limited resources   |
| 10  | Use of analytical taxonomies (categorisation of risk elements and risk events) | Ensuring identification of ‘problem areas’ in processes and the organisation (concentration of risk materialisation causes, etc.) |
| 11  | Approval of the organisation’s tolerance to operational risks (risk appetite) | Implementation of uniform rules stipulating what risks may be accepted, as well as the level of approval of such a decision |
| 12  | An escalation mechanism for contentious issues (including, if necessary, a Risk Management Committee)  | Ensuring a solution is found for contentious situations, which generally arise at the intersection of subdivisions and activity types |
| 13  | Development of risk culture                                           | Ensuring that all employees understand how important it is to manage risks on a systematic basis and take risks into account in their work |
| 14  | Integration with other corporate governance elements                    | Ensuring the maximum efficiency of the entire corporate governance system |
| 15  | Resources (including human resources, financial resources, IT support) | Ensuring the adequacy of the system given the scope and objectives of the organisation |
| 16  | Regulations and other acts on risk management                          | Ensuring that all elements of the risk management system are employed in the organisation |

Implementing each of the elements of the risk management system in view of the goals of their use is ultimately instrumental in minimising losses from the
materialisation of risks, in reducing the resources needed to manage them, and optimising processes, including as a result of addressing cross-functional issues.

It is clear, that solving these problems directly correlates with commercial organisations’ main objective: to survive in the market and maximise profits despite uncertainty and limited resources. Moreover, the larger the organisation is, the greater the effect of a systematic approach will probably be.

**Figure 2. The potential of a systematic approach to operational risk management in a commercial organisation**

| Elements of systematic operational risk management | Final effects | Objective |
|--------------------------------------------------|---------------|-----------|
| Uniform coordinate system                         | Mitigation of loss (damage) caused by risk materialisation | Cost reduction |
| Significant risks                                 | Business process optimisation (costs/benefits) | Income |
| Risk management procedures                        | Resource saving | Increase of financial result |
| Risk appetite                                     |               |           |

Therefore, the main prerequisite for employing a risk management system in the commercial sector is arguably its economic potential. However, this is unlikely to be a determining factor for regulators. Although regulators are commonly considered as financial institutions, they participate in financial markets with a completely different ethos differentiating them from commercial organisations in three critical aspects:

1. *The objectives of their activity* – the functions of the regulator have high social importance. Therefore, their priority in risk management is ensuring that functions are performed properly. Minimising costs (losses) is also important, but is of lower priority.

2. *Resources and powers* – regulators are endowed with special resources and powers in order to perform their specific duties. To that end, their focus in risk management again shifts from minimising costs (losses) to the proper performance of their functions. In terms of resources and powers, the objective boils down more to ensuring a ‘reasonable balance’ of their usage.

3. *Responsibility and accountability* – as a public institution, the regulator is ultimately accountable for its activities to society both directly (through the perception of its activities) and through the existing system of state control, the scope and nature of which differ from the control over commercial organisations.

We can see from these differences that when it comes to regulators, the objective to minimise costs (losses), which is a priority for commercial organisations, does not emerge from the laws of market competition. The
regulator’s risk management system is not monitored by a supervisor, at least not as in the case of commercial organisations.

Nevertheless, as noted at the beginning of this paper, regulators started to actively implement a systematic approach to operational risk management. Therefore, there are arguments in favour of this approach.

### 2.3. Arguments in favour of regulators using a systematic approach to operational risk management

It stands to reason that, if a regulator does not adhere to the general trend of introducing proper risk management, it leads at the very least to discomfort in its interaction with other regulators; it is a matter of authority and common language. If the trend in question is the correct path, then hanging back is also ineffective, as it will be increasingly difficult to get up to speed with each year.

However, analysis shows that this current trend has deep-seated prerequisites that all share the same premise – the specific nature of regulators as socially important institutions.

First, adequate perception of a regulator’s signals in the economy is critical for a regulator to achieve its goals. Its authority plays a key role here. The declaration that the regulator employs best practices (where relevant) when setting certain innovative requirements on supervised organisations is essential for its intentions to be perceived properly and seriously. It is no coincidence that many regulators purposefully declare their adherence to best practices both on their websites and in annual reports.

The Bank of Russia is no exception, publishing its Risk Management Policy on its website⁴ as well as giving brief information on the development of its risk management system in its annual report. This work is also promoted within the activities of the Expert Council on Regulation, Methodology of Internal Audit, Internal Control and Risk Management at the Bank of Russia and Financial Organisations headed by the Bank of Russia chief auditor, as well as the Advisory Council on the Auditing Activities of the Central (National) Banks of the Eurasian Economic Union (EEU) Member States.

However, although this declaration has a positive effect, it will be negated if what happens in practice does not correspond to what is declared. Moreover, confidence in the regulator will be questioned if there is news that the regulator allowed the accumulation of risks that is perceived in the professional environment as unacceptable (leaks of confidential information, signs of corruption, discontinuity in its operations, etc.). It is no coincidence that when such the media publish such news, regulators respond to them almost instantaneously, either with a refutation or with an announcement about measures taken.

---

⁴ See the Risk Management subsection in the Bank of Russia Today section, https://www.cbr.ru/today/risk/
Another argument in favour of regulators using a systematic approach to risk management, which also derives from the underlying premise of the importance of the regulator’s authority, is that in periods of crisis the regulator cannot stay away from current trends. It is no coincidence that after the 2008 crisis, many regulators started to pay greater attention to cost-saving. In such a case, the potential of a systematic approach to risk management for regulators is never more obvious. Moreover, given the scale of regulators influence and the conventionally conservative nature of their activities, this potential is even more pronounced compared to commercial organisations.

Nevertheless, in our opinion, the main argument in favour of regulators employing a systematic approach to operational risk management is the regulator’s role as a risk manager for the financial system, which is associated with the goals of its activities.

Given the fact that any operational risk is the risk of failure to achieve set goals, overall it is possible to say the regulator has only one risk: the risk of inadequate performance of its duties entrusted by law, namely, the duty as risk manager for the financial system.

Therefore, the crux of the regulator’s management of both operational and other types of risks ultimately boils down to minimising risks for the financial system. Even risks of asset loss will ultimately be important in as much as they hamper the achievement of the main goals.

In light of this, the position quite frequently given in economic literature on regulators having economic risks (procurement, managing IT solutions, etc.) is controversial, since all the activities of the regulator are ultimately subordinated to one goal – ensuring that its functions are performed properly. It is not surprising that the risks stemming from support sectors (for example, in IT) often turn out to be higher than those stemming from the main functions.

This was reflected in the speech by the head of the Bank of Portugal, Carlos Costa at a conference on risk management jointly held by the Bank of Portugal and ECB in September 2017 in Lisbon: ‘The art of the central bank is to deal with the risk without losing sight of the two main goals, financial stability and monetary stability’ (Da Silva Costa, 2017).

Returning to the main idea of this subparagraph, it should be noted that to understand the risks of the regulator, we might look solely at one aggregated risk. But this approach is unworkable for the purposes of practical risk management – it is only possible to manage events that are specific, tangible in practice, with clear ‘culprits’, causes, and consequences. Therefore, a regulator’s risks must be understood as an array of specific events in its processes and external environment that may directly or indirectly affect the performance of the function of the risk manager for the financial system. It is only in this context that the significance of a risk can be comprehended.
Thus, the risks for the risk manager performing its functions for the financial system are actually decomposed into what is known as the regulator’s own risks and the risks of its external environment. Here in particular, it is extremely useful to employ a systematic approach to risk management, that enables efficient identification of risks and their specific owners,\textsuperscript{5} assessment of risks and responding to them.

To be clear, this refers only to the regulator’s area of responsibility for monetary and financial stability. The management of the regulator’s financial and strategic risks is also important since their impact on the financial system is subject to special attention.

Nevertheless, given that corporate governance issues are closely interrelated, in recent years there has been a trend towards increasingly blurred boundaries between the elements of corporate governance.

**Figure 3. Arguments in favour of regulators employing a systematic approach to operational risk management**

| Declaration by the central bank (regulator) of its adherence to high standards and best practices in corporate governance | Seeing eye-to-eye with other financial institutions, including central banks (regulators) | Need to use resources of the central bank (regulator) as efficiently as possible, especially during crises | Need for modern tools to best address risk management issues hindering monetary and financial stability |
|---|---|---|---|

3. **Specifics and current issues for regulators employing a systematic approach to operational risk management**

The differences between regulators and commercial organisations that were outlined in the previous section predetermine not only the differences in benefits from a systematic approach to risk management, but also in how the system is set up and is used.

This fact in particular was highlighted by former governor of the Bank of Finland, Erkki Liikanen, in his speech at the aforementioned conference in Lisbon: ‘The area of financial risks is where the special character and responsibilities of central banks probably matter most, making the risk control problems even more complex and nuanced than is the case in ‘ordinary’ banks.’ (Liikanen, 2017). This thesis was conveyed in terms of its applicability to financial risks, but it is clear that it is equally applicable to operational risks.

\textsuperscript{5} Risk owner – person or entity with the accountability and authority to manage a risk (ISO GUIDE 73:2009 Risk management – Vocabulary).
Let us look at the most significant differences in the operational risk management systems employed by regulators and commercial organisations.

3.1. Operational risk appetite

A regulator’s risk appetite is usually low. It is more conservative in its decisions, and the analysis conducted in this paper demonstrably confirms this – it is not the regulator’s aim to constantly take on risks, at least on such a scale and type as commercial organisations do. Moreover, due to the resources and powers the regulator has, taking on large risks may entail negative consequences for the entire financial system.

Differences in risk appetite also mean it is crucial that regulators are cautious when implementing new technologies into their activities and outsourcing their functions. These issues were given special attention at the IORWG conference held in Chile in May 2019.

At the conference, attention was drawn to the fact that despite the benefits of advanced technologies and outsourcing, it is crucial not to neglect the risks they give rise to (including cyber threats, legal risks, data leakage risks). In other words, new technologies and outsourcing can be a source of risks that are no less of a threat and possibly even a greater one. For example, about 70% of regulators use cloud technologies to some extent, but over 15 new risks related to their use have been identified (including loss of control over systems, espionage, hacking, loss of connection, unauthorised access, etc.). In light of this, the conference participants emphasised the need to weigh up the appetite for employing best practices while ensuring continuity of operation, which includes the inclusion of an exit strategy.

However, regulators’ lower risk appetite has its drawbacks – unlike commercial organisations, regulators cannot discontinue certain activities, which means that it is often impossible to reduce the risks associated with them. In such cases, the key objective is monitoring the effectiveness of the measures taken in response to residual risks.

3.2. Approaches to identifying and evaluating operational risks

The crux of the next noticeable difference of operational risk management systems employed by regulators is that their operational risks cannot be viewed in the classical sense – as risks of financial losses. Operational risk is always the risk of deviation from set goals. But when risks are related to qualitative factors, which is the case for regulators, a logical question arises: how can risk be measured, and which negative events in this paradigm can be generally considered significant?

The solution to this problem is to perceive regulators’ operational risk as a negative event that can affect directly or indirectly the achievement of the goals of its activities. In practice, this is accomplished by analysing the processes with
regard to the fact that they involve events that may affect any of the following parameters: operation, reputation and financial assets; the latter is looked into with regard for its influence on the first two.

The depth of decomposition of risks to monetary and financial stability to the regulator’s operations depends on the extent of analysis. Any significant problem can be viewed as a source of or a response measure to a higher-level risk, or can be classified as a separate risk.

**Figure 4. Differences in approaches taken by regulators and commercial organisations to identify and assess risks**

| Commercial organisation | Central bank (regulator) |
|-------------------------|--------------------------|
| Profit making           | Ensuring monetary and financial stability |
| Financial losses        | Damage to business reputation |
| Other risks             | Financial losses*         |
| Impact on operations    |                          |

| Significant operational risks |
|------------------------------|
| * with account of potential impact on operations and reputation |

Clearly, the qualitative nature of regulators’ goals and, accordingly, the approach to identifying its risks, means that the assessment of risks is also of a qualitative nature. As a rule, it involves the use of a five-point scale, which characterises the level of impact the risk has on each of the parameters, using a text description of each of the point levels (to minimise subjectivity). The final score of a particular risk is usually obtained based on a conservative scenario or the weight of each parameter.

The qualitative nature of the regulator goals also implies the need for a qualitative approach to the assessment of the control environment. While suitable approaches to identifying and assessing the risks themselves have already been developed, the problem of assessing the control environment for making decisions on response measures (their contribution to loss mitigation for ensuring proper performance of duties and reputation) is still to be worked through.

There is a similar problem regarding the regulator’s operational risk appetite – it is impossible to assign a quantitative acceptable level to something that cannot be quantified. Therefore, it is only possible to use a qualitative approach here. In light of this, most regulators, including the Bank of Russia, employ an approach that involves determining different tactics and the level of decision-making about the response to risks depending on their level: the higher is the risk level, the lower is the appetite for this risk and the higher is the level of relevant management decisions.

Another noticeable difference in how operational risk management systems are set up in regulators, which is also associated with the qualitative nature of their goals, implies different priorities in the use of risk management procedures.
While registering risk events is of top priority for commercial organisations, regulators use a more proactive approach that relies on self-assessment. In this regard, developing a proactive approach to self-assessment (risks from new processes, projects, and instruments) is a pressing issue.

Furthermore, the qualitative nature of operational risk criteria exacerbates the already long-standing problem for all financial institutions of how to organise registration of risk events. Attempts to establish general requirements, such as registration of all events that have had or may have an impact on operation, have little or no effect: something that is impossible to interpret conclusively, is difficult to fulfil and check.

In view of this, the Bank of Russia has developed an approach to registering risk events based on the high-priority role of self-assessment. It enables identification of significant risks that may become risk events in case of their materialisation. Obviously, self-assessment cannot be used against all possible risks, but the understanding of risks and their consequences that self-assessment provides, aids in better navigating events of all kinds.

**Figure 5. Criteria of risk events in commercial organisations and regulators**

| Operational approach |
|----------------------|
| Commercial organisations |
| Specific criteria |
| Actual (potential) financial losses |
| Other criteria related to financial losses |
| Central bank (regulator) |
| Primarily qualitative criteria |
| Consequences for proper performance of the functions |
| Damage to business reputation |
| Actual (potential) financial losses* |
| Bank of Russia's approach |
| Specific criteria |
| Materialisation of risks identified as a result of self-assessment |
| Other events similar in their impact |

* with account of potential impact on operations and reputation

It is clear that when using this approach, there is the need for a nuanced approach to internal control and audit, namely, non-punishment for a risk event (with focus on evaluating the measures taken) but punishment for a failure to register it.

**3.3. Risk culture issues**

The third and, as we see it, the main difference (and, simultaneously, the most important problem) of operational risk management systems used by regulators is linked to risk culture.

Experts are unlikely to dispute the thesis that it is extremely difficult to explain the need for systematic risk management to owners of the regulator’s risks, as
well as to substantiate that the main benefit of a systematic approach becomes evident at the level of an organisation as a whole. If we add to this the regular workload of the departments, as well as differences in accountability compared to commercial organisations, it is quite easy to understand the situation observed in many regulators when, at best, risk owners see implementing best practices as necessary actions that have nothing to do with them in particular.

Table 3. Main differences in settings of operational risk management systems for regulators and commercial organisations

| Elements of the system          | ‘Root’ differences | Specific features ('settings') of the system | Pressing issues                                                                 |
|--------------------------------|--------------------|---------------------------------------------|---------------------------------------------------------------------------------|
| Risk appetite                  | Lower risk tolerance| A more conservative approach to making decisions on risk response measures        | Weighing up appetite for new technologies and outsourcing while ensuring continuity of operation; developing an exit strategy          |
| Impossibility to discontinue certain activities | Inevitability of accepting high residual risks in some cases |                                                                                   |                                                                                  |
| Risk culture and resources     | The qualitative nature of the main negative consequences of materialisation of the regulator's risks | Qualitative identification and evaluation of risks and the control environment and setting the level of risk appetite | Developing approaches to evaluate the control environment                                                                                   |
|                                |                     | The top-priority nature of self-assessment among all other risk management procedures | Developing a proactive approach to risk assessment (risks from new processes, projects and instruments) |
| Risk culture and resources     | Lower commitment to implementation of best practices among risk owners | The need for top-down support from the directors                                    | Developing non-standard approaches to popularising risk management issues |
|                                |                     | Frequent inevitable conflict of interests with regard to aligning the 2nd and 3rd ‘lines of defence’ (risk management and internal audit) |                                                                                  |
|                                |                     | The significant role of the risk management subdivision |                                                                                  |

The human factor also exacerbates the problem – risk owners are often unwilling to reveal an objective overview of their risks.

In view of this, it is only possible for the regulator to fully implement a systematic approach to risk management, not just on paper but with results, if two conditions are met simultaneously.

The first condition is the comprehensive top-down administrative support of senior directors. When it comes to regulators, as well as other socially important institutions, the fundamental truth about top-down support manifests itself most clearly (Committee of Sponsoring Organizations of the Treadway Commission, 2009). For this reason, the unit for coordinating operational risk management, despite the functional conflict of interest with internal audit, is often established and at the earliest stages functions within the internal audit department.

The second condition is the availability of sufficient human resources and IT solutions in order to implement and maintain the operational risk management...
system, with a particular priority put on trained specialists in the centralised unit who will coordinate operational risk management. Specialists in risk management and the regulator’s processes are needed to convey the information given in this paper to other staff.

Regulators’ practical experience shows that a ‘box ticking’ approach to organising operational risk management, where risk owners do not get sufficient immersion and coordination from the risk management subdivision in order to fulfil risk management requirements, bears no result. Subsequently, questions arise about the justification of the costs of maintaining the system.

In this vein, it becomes increasingly important to promote the efforts aimed at developing a risk management system. Increasing attention should be paid not only to explanations about the benefits of a systematic approach, but also to stimulating the interest and involvement of staff in this aspect, generating a positive attitude towards it. For example, joint brainstorming sessions of subdivisions about responding to non-standard large-scale risk events, regular digests of the risk management subdivision for the directors including information about past risk events, various competitions and other initiatives.

4. Trends and prospects for further development of operational risk management employed by regulators

The fact that regulators have built up two decades of practice in employing a systematic approach to operational risk management means we can talk about certain trends and prospects in this field.

They include the aforementioned development of a risk culture and increased attention to the risks from new technologies and outsourcing. Regulators are also paying a lot of attention to automating operational risk management procedures. The integration of operational risk management with other elements of corporate governance is taking on an increasingly distinct shape.

**Figure 6.** Main trends in developing a systematic approach to operational risk management employed by regulators.

We can observe the trend towards integration in a whole range of corporate governance elements.

Thus far, the issues of how operational risk management is interrelated with internal control and internal audit, including within the practical implementation
of the ‘three lines of defence’ model, are probably the only ones to have been worked out most thoroughly. The remaining areas are at various stages of studying the fundamental aspects of their integration.

Integration with financial risk management can be highlighted among these actively developing areas. From the functional point of view, the reasons behind this trend are not obvious, given the differences in methodologies, but integration at the organisational level is no longer a rarity. Such decisions are generally taken in order to avoid the conflict of interests when one subdivision of the regulator combines financial risk management functions and operations related to risk acceptance, as well as because the directors prefer to be informed about all of the regulator’s risks by a single source.

Another widespread trend is to combine operational risk management with ensuring continuity of operation (COOP): over 50% of the regulators that are IORWG members have taken steps to integrate these issues. This trend is not only of organisational, but also of a clear methodological nature since both of these systems (that is, operational risk management and COOP) deal with operational risks.

The fundamental difference is as follows. Operational risk management focuses on preventing risk materialisation, i.e. deals with mainly preventive measures. COOP system’s objective is to identify the most critical operational risks that, should they materialise, threaten the performance of the regulator’s critical functions, and to proactively develop measures that would ensure prompt recovery of operation to the extent and quality required in case of risk materialisation.

The integration of operational risk management with process management is underway – about 70% of the IORWG members have already taken steps in this direction. They include the Bank of Russia, whose operational risk management system is based on a process approach. Using process management significantly eases the task of risk identification and allocation of responsibility for risks. The operational risk management system, in turn, aids in more accurately determining the boundaries of processes and identifying the potential for their improvement.

Furthermore, in the course of developing operational risk management systems, those putting them into practice gain an understanding of another important issue – the relationship between operational risk management and strategy. The more risk management develops, the closer these ‘sensitive matters’ are.

A key event in this field was the COSO publication ‘Enterprise Risk Management – Integrating with Strategy and Performance’ in 2017 (Committee of Sponsoring Organizations of the Treadway Commission, 2017). The report looks at the three main aspects of the relationship between operational risk management and strategy: managing risks that impede the implementation of the chosen strategy, the need to take into account risks when choosing a strategy, and risks of inconsistencies in the strategy in terms of the mission, the vision, and values of the organisation.
It can therefore be seen that, the integration of operational risk management with other elements of corporate governance is in the development stage. The obvious potential of such integration means that there is a considerable opportunity for further in-depth study of the related issues.

5. Conclusion

In terms of operational risk management, all regulators can be currently divided into two main groups.

The first group that most regulators belong to has already introduced or is in the final stage of introducing a systematic approach to operational risk management. The regulators in this group have acknowledged the usefulness of using a systematic approach earlier than others and, as a result, are already benefiting from its introduction while they continue to improve it and set trends in this field.

The second group includes those regulators who have not yet made a decision regarding the feasibility of employing a systematic approach or are using it in a fragmented and/or formalistic way. Owing to the aforementioned differences from commercial organisations, these regulators do not bear critical risks that may result from such stance. One way or another, they do manage their risks, albeit in an intuitive and less effective fashion.

Yet, returning to the idea that the art of a regulator is to manage risks without losing sight of monetary and financial stability, it is essential to remember the key role of the regulator’s authority that largely depends on whether the regulator itself is able to use and adheres to the approaches that it demands from the market.

This paper also demonstrates that an operational risk management system is a useful tool for identifying and directly managing risks that can ultimately prevent the regulator from achieving the goals of ensuring monetary and financial stability. It is also a tool for ensuring a reasonable balance between the extent of control environment and the costs of its application.

Furthermore, the rationality of a wait-and-see position in relation to the ongoing evolution of this field can only be partially corroborated. It is only the basic parameters of the system that are loosely the same for everyone, while the fine-tuned settings are determined by the conditions of operation of a particular regulator, which is often revealed in the course of implementation of the system.

It is also impossible to instantly ensure the emergence of the main element of an effective operational risk management system, a mature risk culture. It takes many years for regulators to establish this culture.

In the opinion of the author, the analysis conducted in this paper confirms the justifiability of the trend towards the use of a systematic approach to operational risk management by regulators. It also confirms the fact that it is impossible
to achieve results from its use without paying increased attention to the issues highlighted in this paper, where risk culture issues come to the fore.

References

107th United States Congress (2002). The Sarbanes-Oxley Act.

Bank for International Settlements (2009). Management of Non-Financial Risks. In: Issues in the Governance of Central Banks: A Report from the Central Bank Governance Group. Basel: Bank for International Settlements, pp. 151–161.

Basel Committee on Banking Supervision (1997). The Core Principles for Effective Banking Supervision.

Committee of Sponsoring Organizations of the Treadway Commission (1992). Internal Control – Integrated Framework.

Committee of Sponsoring Organizations of the Treadway Commission (2004). Enterprise Risk Management – Integrated Framework.

Committee of Sponsoring Organizations of the Treadway Commission (2009). Effective Enterprise Risk Management Oversight: The Role of the Board of Directors.

Committee of Sponsoring Organizations of the Treadway Commission (2013). COSO Issues Updated Internal Control – Integrated Framework.

Committee of Sponsoring Organizations of the Treadway Commission (2015). Leveraging COSO Across the Three Lines of Defense.

Committee of Sponsoring Organizations of the Treadway Commission (2017). Enterprise Risk Management Integrating with Strategy and Performance.

Committee on Corporate Governance (1998). Committee on Corporate Governance: Final report. London: Gee Publishing.

Committee on the Financial Aspects of Corporate Governance (1992). The Financial Aspects of Corporate Governance: Final Report. London: Gee and Co., Burgess Science Press.

Da Silva Costa, C. (2017). Risk Management for Central Banks. [Speech] Joint Bank of Portugal and European Central Bank Conference on “Risk Management for Central Banks”, Lisbon, 25 September. Available at: https://www.bis.org/review/r170928b.pdf [accessed on 15 October 2019].

Higgs, D. (2003). Review of the role and effectiveness of non-executive directors. London. Available at: https://ecgi.global/download/file/fid/9424 [accessed on 15 October 2019].

HM Treasury (2004). The Orange Book: Management of Risk – Principles and Concepts.

Institute of Chartered Accountants in England and Wales (1999). Internal Control. Guidance for Directors on the Combined Code. London: Institute of Chartered Accountants in England and Wales.

Khan, A. (2016). Central Bank Governance and the Role of Nonfinancial Risk Management. IMF Working Paper, N 34.
Liikanen, E. (2017). *Central Banking and the Risk Management of Central Banks – What Are the Links?* [Speech] Joint Bank of Portugal and European Central Bank Conference on "Risk Management for Central Banks", Lisbon, 26 September. Available at: https://www.bis.org/review/r170929b.htm [accessed on 15 October 2019].

Myners, P. (2001). *Institutional Investment in the United Kingdom: A Review.*

Organisation for Economic Co-operation and Development (1999). *The OECD Principles of Corporate Governance.* Paris: OECD Publications.

Study Group on Directors’ Remuneration (1995). *Directors’ Remuneration: Report of a Study Group Chaired by Sir Richard Greenbury.* London: Gee Publishing.
3rd Bank of Russia International Research Conference
Monetary Policy, (Macro-)Prudential Regulation and Their Interactions

July 7–8, 2020, St. Petersburg, Russia

The scientific committee of the conference is comprised of the Research Advisory Board of the Bank of Russia. This conference will bring together researchers from academia, central banks, and policy institutions.

Submission topics:

→ **We invite submissions on relevant topics, in particular (but not limited to) the following:**

  • Co-ordinating monetary and prudential policies
  • Efficient communication and optimal central banks’ openness
  • Monetary policy under (model/scenario/parameters) uncertainty and optimal monetary policy
  • Implications of the International Monetary System for optimal monetary and macroprudential policies in emerging markets and advanced economies. Monetary policy trilemma and dilemma, optimal foreign exchange intervention, optimal capital controls
  • Co-ordinating macroprudential policy with traditional risk-based regulation of financial institutions
  • The impact of commodity prices on general inflation and systemic risk, and the appropriate policy responses
  • Implications of (income/regional/demographic) heterogeneity for the formulation of monetary and financial stability policies
  • Encouraging socially efficient financial innovation without sacrificing financial stability. Market competition, ”too big to fail” and sustainability of financial institutions: policy implications
  • Business models, risks and corporate governance in banking with implications for prudential regulation and supervision
  • Challenges for prudential regulation and supervision in financial institutions
  • Interaction of central banks’ policies and fiscal policy

→ **To submit a draft paper,** please send it to board@cbr.ru, putting “Bank of Russia Conference 2020 Submission” in the subject line and include the following information: full name, affiliation and position in the institution you represent.

→ **The closing date for submissions is March 1, 2020**
Authors whose papers have been accepted will be notified by April 1, 2020

→ The organisers will reimburse travel and accommodation costs for presenters and discussants taking part in the main and supplementary sessions

Conference participants will be informed of the possibility to publish their papers in the Bank of Russia’s journal *Russian Journal of Money and Finance*, an open access peer-reviewed academic journal.

Please see more information regarding the programme and organisational details:
cbr.ru/eng/ec_research/2019-12-11_call/
Call for Papers

The Bank of Russia and the Russian Journal of Money and Finance invite students and PhD fellows to submit papers for the 2nd Economic Research Competition.

Submission topics:
- Central bank's policy
- Inflation
- Financial stability
- Banking
- Data analysis: methodology and results

Key requirements for the research:
- Applied research
- Meeting academic criteria
- The study should have been carried out no earlier than 2017
- When carrying out the research, the author should have possessed a Bachelor's or Master's degree, or else been working towards a PhD

How to apply:
1. To submit a paper in Russian or English, please send it to journal@mail.cbr.ru, putting “Application for 2020 Bank of Russia Research Competition for students and doctoral researchers” in the subject line.
   Give your full name, course of study, and educational institution.
2. A cover letter, containing the research objective, the contribution made by the authors (the originality of the results when compared against specific existing studies), results, and conclusions.

Papers are accepted in PDF format (file size not more than 5 MB).

Competition dates:
The closing date for submission is 15 May 2020.
The winners will be announced on 15 June 2020.

Competition jury:
Editors and the Editorial Board of the Russian Journal of Money and Finance.
Researchers from the Research and Forecasting Department, the Monetary Policy Department, and the Financial Stability Department of the Bank of Russia.

Publication of research papers:
The Russian Journal of Money and Finance will consider the winners’ papers for publication.

The competition winners will be invited to participate in the Bank of Russia Macroeconomics Summer School, the Bank of Russia International Conference, and the International Financial Congress held on 7–10 July 2020 in St Petersburg (travel and accommodation costs covered).

For more detailed information, please see cbr.ru/eng/ec_research, rjmf.econs.online/en.