Permanent Control: The Formula of a Sound Operational Risk Management Approach in the Albanian Banking System

Mag. Dott. Ardita Todri

Faculty of Economics, Elbasan
University of Elbasan "Aleksander Xhuvani", Elbasan, Albania
E-mail: ardita.todri@gmail.com, Mobile:+355 692841581

Mag. Dott. Valbona Dudi

Faculty of Economics and Political Sciences
Catholic University "Our Lady of Good Council",Tirana, Albania
E-mail: valbona.dudi 01@libero.it, Mobile:+355 672004704

Abstract

Statistically based the operational risk management culture is still primitive in the Albanian banking system and that's why it attracts and causes operational risk. Inevitably, the operational risks may only be increasing, as we see growing globalisation, more competitive markets, rapid developments in technology, and periods of economic difficulty... by becoming an emergency for the Albanian banking system. Thus, in this paper we explore on proposing to a/m system a developing strategy for detection, prevention and response to the operational risk with highest standards of professionalism and the utmost integrity in dealing with all stakeholders of the Albanian banking system by providing also to its customers a safe banking business guaranteed from the banks control functions.

1. Introduction

It should be admitted that operational risk management remains a very individual issue pertaining to each bank in Albanian banking system in prospect of business, customer target group, organisation, etc.... and finally to the perceived development strategy. This led us to discuss the matter initially with risk professionals of banking industry aiming to categorize the concerns faced and latter on think about appropriate responses materialized through proposed methodologies needed to be implemented aiming a proactive general operational risk management in the a/m system. It's worth mentioning that specific nature initiatives are undertaken from Albanian Association of Banks through the establishment of technical committees but anyway it seems that were not enough.... Precisely, by enabling a broader discussion of the issue based not only on loss statistics but also to the overall operational risk management process, were verified problems in operational risk events identification, assessment and analysis due to the lack of detailed controls exercised permanently on the entire banking activity and following their miscommunication to the responsible instances.

1.1 Data Collection Methodology

Our analysis used qualitative and quantitative data collected directly from the second level banks. For this purpose, it was elaborated a structural questionnaire with specific questions (regarding the operational risk management methodology deployed in the bank and respective loss statistics) which was electronically delivered to the Risk Management departments (by making clear the data usage, anonymity preservation and by simultaneously requesting the response validation from Chief Risk Officer before the submission). In any case the data collected were analysed by using SPSS-16 version in terms of validity and reliability.

1.2 Research Results

The questionnaire through which the analysed data were collected was organised in two parts .The first part consisted in questions on the existing daily operational risk management approach (regulatory framework or the group standards) while the second one referred to the defective areas statistics (operations, market and lending) revealed during the last two years (since the regulation of operational risk management from Central bank of Albania became effective).

The responders were asked to mark the level of daily operational risk management process on a 5-point scale in the first part while a 3-point scale was used in the second part regarding the severity of loss in each defective area.

This research results have shown that in the first part, banks mainly handle the risk management according their headquarters' standards /requirements in the quality of the international banking groups affiliates by including our regulator's embryonic requirements. Furthermore, the second part results revealed not fully compliant with the operational risk approach implemented from the banks, so more operational risk events were reported in the areas not indicated under the methodological framework implemented. Logically, these results bring to strong arguments on deeper controls climate in each cell of the operational risk management process powered by permanent control functions.

2. Tracking operational risk events through warning signals and alerts captured from control lines

Even why operational risk identification and reporting mandatory remains the responsibility of each bank employee it can't be correctly handled due to the human being nature. Under this context the identification process should be resized by using different warning signals and alerts received from the key risk indicators (KRI's) as well as by implementing first and second control levels in the banking activity. *What are the key risk indicators, and what can be treated as operational risk warning signals and alerts*?

KRIs (*see Fig.1*) are measurable metrics/scorecards or indicators that track exposure or loss, or, as one person put it, "trouble". The indicator becomes key when it tracks an especially important exposure, or it does so especially well, or ideally both. There is a rationale for thinking that, at least in some ranges, changes in the value of this indicator are likely to be associated with changes in operational risk exposure or operational loss experience.

While warning signals encompasses: business risk, cultural, management, employee, process, transactions, financial, environmental risk and IT - data risk issues.

And operational risk alerts consist in: unusual destinations, discrepancy between earnings and lifestyle, unusual irrational or inconsistent behaviour, alteration of documents and records, extensive use of correction fluid and unusual erasures, photocopies of documents in place of originals, immediate fluctuations in stock accounts, etc.

By this way, in order to reflect and capture on time the warning signals, alerts and translate them in KRIs we should affirm and extend the first (1.1C) and second (2.1C) control levels. In other words, we should divide the banking practices in two phases (through the access rights matrix), in operative (1.1C) and approval one (2.1C) on behalf of its criticism and risk exposure. Furthermore, the experience obtained from the two-phase validation process as bureaucratic seems as well as risk identifier appears. The approval phase also can increase the chances to retrieve additional warning signals, alerts and contributes in the improvement of operational risk identification methodology by contemporary enhancing the internal communication. An important fact in the identification process is the causality but should be mentioned that the periodic controls (internal, external audit and permanent controls) can also reveal them. And sometimes the last requires the process resizing.

Fig 1. KRI evaluation method

$$KRI = \frac{\text{Anomalies/Breaches/ Failures identified}}{\text{Total no of transactions controlled}}$$

Source: Risk Management Association (RMA)-http://www.rmahq.org/RMA/.

3. Operational risk investigation scheme

All the operational risk events revealed through the 1.1C and 2.1C controls should be investigated in order to understand the cases which made the occurrence and prevent similar future events. For the a/m purposes the following investigation scheme is proposed:

E-ISSN 2281-4612
ISSN 2281-3993

Academic Journal of Interdisciplinary Studies
MCSER Publishing, Rome-Italy

Vol 2 No 8
October 2013

➤ Preservation of evidence (Physical and Electronic);
➤ Interviews;
➤ Statements and witnesses;
➤ Statements from suspects;
➤ Analysis of the Whistle Blowing Policy (compliant settled on a malpractice noted) ;
➤ The 2.2C and 3C controllers reports on the issue.

In respect of the investigation steps and respective results should be implemented the recommendations of the 2.2C and 3C controllers which may consist in further 1.1C, 2.1C and 2.2C controls implementation or in additional preventive measures in respect of anomalies observed.

4. Operational risk monitoring and assessment

Operational risk monitoring is the crucial point of the entire operational risk management process. It should be widespread in the eight indicated business lines/functions as well as on operational risk categories according to Basel II methodology and must be exercised in quarter, semi-annual and annual basis. The quarterly monitoring is performed against through KRIs , while the semi-annual through 2.2C and 3C level of controls. These controls are exercised from the control functions, respectively the 2.2C level of control is exercised from the Permanent Control Department while 3C level of control is exercised from Internal Audit Department. In contrast to 1.1C and 2.1C level of controls they are exercised on sample basis. Based on these control results and relative experience Permanent Control and Internal Audit Departments can give indications on new KRI's establishment in order to improve the monitoring process as well as to evaluate the necessity to build and exercise additional 2.2C level of controls. These practices used among banks can enable the interpretation and comparison of KRIs between them by expanding their external communication line. The assessment refers to a three dimensional model (risk function, risk category and business lines (*see Fig. 2*) for the overall institution as well as for a certain product or activity within the bank

Fig.2. Three dimensional model (Business Functions & Lines and Risk Categories
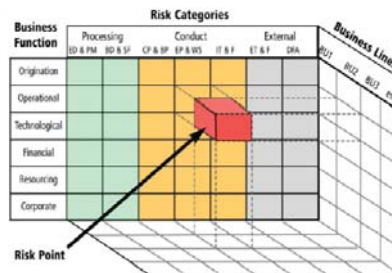
Source: Risk Management Association (RMA), http://www.rmahq.org/RMA/.

This process must be held at least annually, thanks of the business lines manager's (senior managers) contribution in the quality of the main responsible for operational risk management in the respective area. Organized under monitoring and assessment workshop theme may be exploited the occasion to build and develop scenarios that can impact the business under different banking areas expert's knowledge. And, this kind of communication aims on a general awareness toward the collaborators by contributing on a safer internal environment.

5. Segregation of duties

The segregation of duties is quite expensive for banks as more people are needed to accomplish and finally execute the initiated transactions. It largely depends from bank's core systems designation or their strategic choices related to process centralisation or decentralisation. In any case the segregation of duties perfects the transactions quality and can raise their quantity due to the operations homogeneity. Therefore large banks always segregate the duties (implement the four eyes principle) in order to correspond to the business needs (*a practical context*) and from the other side the

segregation of duties makes the people involved in the system more responsible of the actions undertaken (*a philosophical context*). The segregation of duties reveals more than necessary for the operational risk management process as assists in the identification of anomalies and urges their management. Exactly, the anomalies identified from the segregation of duties in any other manner can be treated as key performance indicators (KPIs). Furthermore, the key performance indicators may be used as operational risk warning signals or alerts retrieved to better understand and evaluate the institutions operational risk situation. Thus, the segregation of duties represents an alternative way of exercising different level of controls by becoming a real internal preventive mechanism.

6. Permanent control structure

Permanent control functions (the specialised second level controls-2.2C), adjusted to specific needs are lately introduced in banking control philosophy. They are perceived to supervise the transactions /processes finalized through first or second level of controls (*see Fig. 3*).

Fig.3: KPI evaluation

$$2.2c \text{ indicator/ KPI} = \frac{TRN's \text{ performance}}{Controlled \text{ sample}}$$

Source: Permanent control function, Calyon, http://www.ca-cib.com

Shortly, they ascertain the validity of segregation of duties within the institution by using against the four eyes principle logic and giving as feedback key performance indicators (KPIs). Prone on more sensitive areas such as: compliance, legal, operational risk, financial risk, accounting risk, credit risk, outsourced essential services and IT security areas they cover the major part of banking activity (*see Fig.4*).

Fig.4: Permanent Control Hierarchical Sceme
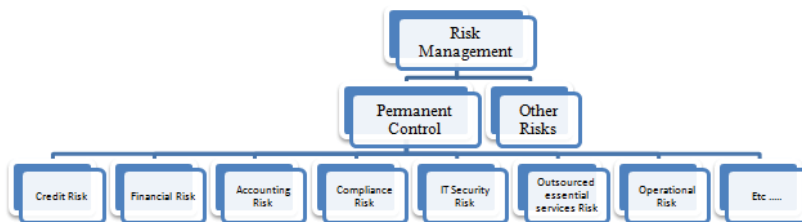
Source: Permanent control function, Calyon, http://www.ca-cib.com

However they can be further expand in the same/different, directions if it deems necessary. Predominantly, they are quarterly, semi-annually and annually exercised in respect of the controlled transactions/ processes frequency. In contrast to audit controls, they are performed in distance from the appointed persons/ controllers (in a/m area) but anyway in sample basis. All the controls conducted must be trialled in order to give to the validator (head of permanent control) the possibility to recheck the databases build from the controllers before giving the final consent according to the calculation of KPIs rating. Nevertheless the experience accumulated on the controls typology provides changes on the KPIs rating. Thus, their evaluation limits on low (green), medium (orange) and high risk (red) may change on behalf of banking areas procedures/policies as well as business environment and expectations. In any case these results carry information above anomalies in the controlled areas by indicating the necessity of investigations in place (verifications), which may further lead in measures on the transaction/process procedure review or establishment of additional 2.2C level of controls regarding the mentioned process.

7. Follow-up the permanent control results

To follow the permanent control results means:
- ➢ to identify (the reasons that generate anomalies);
- ➢ monitor the correction of anomalies that lead to potential operational risk events.

Obviously special attention is paid to the medium and high risk rated areas, and the most direct way to follow-up the issues derived from a certain process is to discuss above defective chains of the process with the direct area's responsible/ senior manager. This discussion can help the area's controller to understand the irregularities reasons and request the appropriate adjustments. For this purpose an action plan must be designed and launched (with a timeframe) from the controller in request of the corrections conduction. The solely responsible for the initiated action plans and respective completion is against the controller. The results achieved from all the initiated action plans status are reported in Operational or Fraud Risk Committees by being subject of the decision making process regarding further measures to be undertaken under operational risk management approach. Therefore, permanent control follow-up is a mutual process between control and execution lines that monitors the last aiming to cover the irregularities by contemporary educating them. Thereby the internal communications strengthen and reduce the operational risk events non–response chances.

8. Permanent control instruments in support of Operational Risk's Advanced Measurement Approach implementation

The underlying idea of Advanced Measurement Approach (AMA) represented from Basel II Framework is that banks use their internal models to estimate the necessary capital for operational risk management, which would align it with economical capital. By this way, using AMA instead of other much simpler alternative approaches in operational risk management such as Basic Indicator Approach (BIA) and Standardized Indicator Approach (STA) it can be allocated a lower capital charge related.

As known, the implementation of AMA requires the fulfillment of a lot of preconditions from the institutions (*see Fig. 5*) and the major part of the second level banks operating in Albania could not be expected to meet them for years especially when regulatory requirements regarding operational risk management are basic.

Fig. 5. Typical approach to build an LDA model, Source: Alexander, C.(2003).*Operational Risk: RAM. PHFT.*
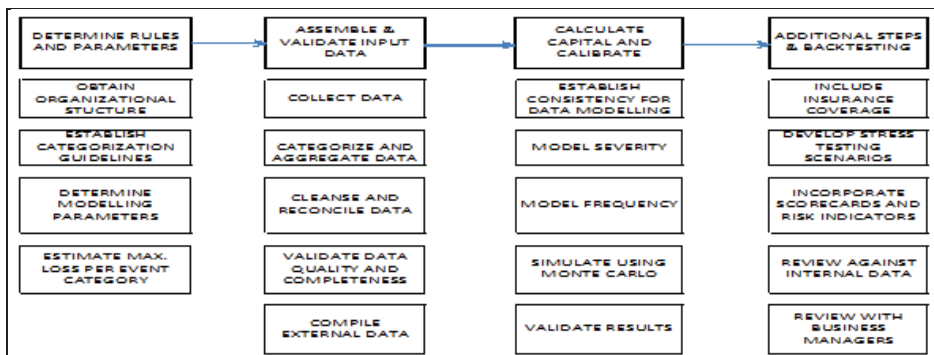
But it should be also considered that, generally the operational risk quantification as per AMA's requirements is still a difficult task for the time being due to: data shortages, the nature of operational risk and lack of a strongly risk-sensitive exposure measure in operational risk modelling. Anyway the major part of the banks in the albanian banking system are trying to make a step ahead regarding the own operational risk management as per respective group requirements.

8.1 Internal Data Collection Process

For the first time Albanian banking system started to collect and report the respective loss events data for Bank of Albania (BoA) on July 2011, even the loss data collection process had already started as a necessity of international banking groups operating in Albania through respective affiliates (but none of them has actually more than 3 years of loss

historical data as revealed from the questionnaire results). The internal loss data collection process assumes that historical losses are a good indicator for predicting future losses, meaning that the risk management process keeps them equally, and in fact this is difficult to be guaranteed. In any case is necessary a large set of data with a certain number of losses for a consistent measurement, but more losses can be revealed through a sound exercise of permanent control.

8.2 External Data Collection Process

From the other side is quite impossible to exchange the loss data in the Albanian banking system without having a loss data pool (it should be the regulator's responsibility to collect and make available these data to the entire system) but it remains still a prospective.

It should keep in mind the problematic of external data usage as argued from Allen and Bali (2004), that operational risk datasets tend to suffer from under representation of low frequency, high severity events and from the respective confidentiality, even are mandatory to be reported. Under this context the problem can be solved by using a common data pool as previously mentioned (which should be developed and managed from the regulator based on loss data collected from the banks aiming to share the same risk factors such as : business activity, size, business and control environment, etc.) which will be useful to the system itself.

Despite this fact the risk data gathered during an economic expansion can't be used in a recession period. But anyway, it should be underlined that the establishment of a data pool is an emergency for the regulator in order to support and manage not only the loss data collection process but also to make aware the Albanian banking system for the respective operational risk size. However it doesn't represent consistency with each bank operational risk's profile as mainly operational risk events are considered uncorrelated. In fact, mainly AMA is a loss distribution approach (LDA) which depends on internal and perhaps on external loss data, whereas the other techniques are used to supplement the historical loss data they are also required to be implemented.

Furthermore the view held by Haubenstock and Hardin (2003), argue that the LDA utilizes internal and external data but it involves additional steps, including the development of scenarios for stress testing and incorporating scorecards and risk indicators.

Later on, regarding the LDA, Hausebenstock and Hause (2006) suggested that it may be used for the whole firm, whereas scorecards can be used for business lines (which they call a hybrid approach) and the issue here refers to the loss allocation in the business line's in case of multiple losses and in this respect permanent control plays a very special role.

8.3 Scenario Analysis

The scenario component of an operational risk model is predominantly determined by two steps: the definition of scenarios and their calibration. For both of these tasks, an integration of expert judgment for tailoring the scenarios to the bank's operational risk profile is a common approach. However, expert judgment should only complement industry information instead of totally replacing it. In particular, industry information on tail distribution characteristics of common scenarios contains significantly more robust information than an often arbitrary expert calibration at high severity quintiles.

The definition of scenarios should cover all potential high severity risks (assessed during monitoring) and result in a longer term-invariant of the model. The tail calibration of scenarios is pre-dominantly a mid-term invariant "worse cases assessments should no change frequently", however it requires at least a yearly review based on the current business environment and on the information collected. Problems are also associated to the scenarios analysis, the scenario elaboration process requires significant resources including the direct participation of a broad range of senior managers to understand the scenarios that could impact the business. The scenarios almost are built by using empirical expert's knowledge of different banking areas.

At the current stage for the Albanian banking system the scenario development perception is a very complicated process which represents just a potential loss initiating from the fact that operational risk losses are considered uncorrelated and there is no memory related due to a proactive operational risk management. It is considered a novelty for the Albanian banking system which remains still on theoretical terms of scenario development, therefore somehow questionable but specifically the matter can be further explored and managed from a pervasive permanent control context.

8.4 Business Environment

Business environment and internal control mechanism should be defined by Top Management with a list of Key Risk Indicators (KRI's) and Key Performance Indicators (KPIs). Both are classified considering their impact on operational risk by using scorecard. The scorecards usage for AMA implementation is subjective as they are typically mapped in a subjective manner to monetary loss amounts, particularly in case of human risks (inadequate or failed people or management processes). The KRIs and KPIs identification requires an intensive dedication to the business lines through proactive control mechanisms aiming to capture the gaps in order to establish the most important representatives that should be analyzed for operational risk events mitigation purposes.

That's another complex approach considering the typology of operational risk events in different business lines. On the other hand there isn't any benchmark in place in the system regarding KRI's and KPIs typology even for the eleven KRIs established to be reported and monitored from our regulator and that's why the integration of the KRIs and KPIs data in the bank's operational risk management process is difficult concerning to the external data comparison and usage. In any case, it should be admitted that the data collected from the permanent control function in our banking environment can enhance the benchmarking through the implementation of standardized controls strategy by considering also the operational risk data pool establishment and usage.

9. Conclusive remarks

As observed, permanent control function affects every cell of the operational risk management process by simultaneously increasing the communication, given that it penetrates to the heart of the matters.
In fact, permanent control becomes integrative part of operational risk management as:

> ➢ Increases operational risk events identification chances;
> ➢ Examines the overall banking activity independently from its segment's risk profile;
> ➢ Implements horizontal and vertical monitoring schemes;
> ➢ Proactively prevents by establishing specific standards on risk awareness culture;
> ➢ Follows-up the defective areas by implementing Corrective Action Plans,

by substituting the last three steps of Operational Risk Management Cycle as argued from Hussain (2000) and consisting in the reduction of operational risk events probability and severity.

Obligatorily, it constitutes a dynamic and complex function since involves people, processes, targets, etc against a certain expenditure depending on the bank 's size (as it can be traditionally exercised or managed through particular systems) and represents the management weapon and senior management task.

It gives the right indications for risk transfer mechanism implementation (insurance), processes, procedures, and strategy redesign if they reveal defective.

Moreover the permanent control series makes available important elements of the Operational risk Advanced Measurement Approach such as: KRI's, KPI's, scenario analysis, internal loss data benchmarked with the external loss data, etc.

By this way, it promotes the banks to spontaneously explore the internal modelling independently from the regulator's standards set with lower costs primarily in view of respective needs and goals...

And finally attempting the gradually switch in the Operational risk Advanced Measurement Approach, of course if it deems convenient for the banks itself. In principle, permanent control is a good portent for operational risk management as it will reduce the cost of doing business in the second level banks pertaining to the Albanian banking system considering the actual circumstances.

References

Alexander, C. (2003). Operational Risk: Regulation, Analysis and Management. ISBN:978-0-273-65966-2
Allen, L. and Bali, T.G. (2004). Cyclicality in Catastrophic and Operational Risk Measurements, Working Paper, City University of New York, September.
Bank of Albania(2011). On the Operational Risk Management Regulation.
Available:http://www.bankofalbania.org/web/Regulation_On_the_operational_risk_managment_6063_2.php?kc=0,28,0,0,0 (January 19, 2011).
Bessis. J. (2011). Risk Management in Banking (Third Edition). ISBN: 0470689854.
BCBS (2006). Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework -

Comprehensive version, Available: http://www.bis.org/publ/bcbs128.htm (June, 2006).

Credit Agricole (Calyon), Available: http://www.ca-cib.com.

Coleman, S.Th. (2011). A Practical Guide to Risk Management. ISBN: 978-1-934667-41-5.

Haubenstock, M. and Hardin, L. (2003). The Loss Distribution Approach, in Alexander, C. (ed) Operational Risk: Regulation, Analysis and Management. ISBN:978-0-273-65966-2.

Hausebenstock, M. and Hause, J. (2006). Practical Decisions to Successfully Model Operational Risk, in Davis, E. (ed) The Advanced Measurement Approach to Operational Risk. ISBN: 1 904339 88 3.

Hull, C.J. (2012). Risk Management and Financial Institutions (Third Edition). ISBN: 978-1-118-26903-9.

Hussain, A. (2000). Managing Operational Risk in Financial Markets,Butterworth-Heinemann,Oxford. ISBN: 0 7506 4732 9.

Kaiser, T. and Kohne, M. (2006). An Introduction to Operational Risk. ISBN: 1 904339 51 4.

Klugman, A.S., Panjer, H.H., and Willmot, E.G.(2012). Loss Model: From Data to Decisions (Fourth Edition).
 ISBN: 978-1-118-31531-6.

Moeller, R.(2010). IT Audit, Control , and Security (Second Edition). ISBN -10: 047140676.7.

Nash, R.A. (2003). The Three Pillars of Operational Risk, in Alexander, C. (ed) Operational Risk: Regulation, Analysis and Management. ISBN:978-0-273-65966-2.

Pezier, J. (2003). A Constructive Review of the Basel Proposals on Operational Risk, in Alexander, C. (ed) Operational Risk: Regulation, Analysis and Management. ISBN: 978-0-273-65966-2.

Rao, V. and Dev, A. (2006). Operational Risk: Some Issues in Basel II AMA Implementation in US Financial Institutions in The Advanced Measurement Approach to Operational Risk. ISBN: 1 904339 88 3.

Rebonato, R. (2007). The Plight of the Fortune Tellers: Why We Need to Manage Financial Risk Differently. ISBN-13:978-0-691-13361-4.

Risk Management Association (RMA), Available: http://www.rmahq.org/RMA/.

Scalera,F.,Todri,A.(2012). The operational risk evaluation and management prospective in the Albanian banking system. 1st International Conference "South –East European Countries towards European Integration" Elbasan (Albanian), 20th October 2012, ISSN : 2221-5956.

Scalera,F.,Todri,A.(2012). "Why the implementation of the Advanced Measurement Approach in Operational risk management isn't a so good idea : The Albanian banking system case", International Journal of Business and Commerce Vol.1, No.12: August 2012[47-55], ISSN: 2225-2436.

Todri, A., Shingjergji, A. (2012). The internal control culture in the Albanian banking system under fraud prevention context, 1st International Conference "South –East European Countries towards European Integration" Elbasan (Albanian), 20th October 2012, ISSN : 2221-5956.