Available online at www.sciencedirect.com

ScienceDirect

Procedia Economics and Finance 26 (2015) 800 – 805

Procedia Economics and Finance

www.elsevier.com/locate/procedia

4th World Conference on Business, Economics and Management, WCBEM

Monitoring of compliance risk in the bank

Ewa Losiewicz-Dniestrzanska[a]*

[a]*Wroclaw University of Economics, Komandorska Street 118/120, 53-345 Wroclaw, Poland*

Abstract

One effect of passing through the world financial crisis is to pay closer attention to compliance with the regulations of business by banks and other financial institutions. In recent times there has also been an increase in the importance of compliance units involved in the management of compliance risk in the bank. The author in the paper highlights the need to risk monitoring of non-compliance with the regulations and presents some monitoring tools of this kind of risk in the bank. Examples of tools and techniques presented in the paper relate to banks operating in Poland. These are mainly methods based on using indicators, supported by information technology tools for business process management. The scope of compliance evolved last years to a much broader area. The author of the paper draws attention to the growing popularity of the approach integrating operational and compliance risk

© 2015 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Peer-review under responsibility of Academic World Research and Education Center

Keywords: compliance in a bank; compliance risk monitoring; monitoring tools, indicators, risk maps

1. Introduction

The importance of compliance in banks of the world is increasing. Both banks themselves and regulators emphasise t After the crisis of 2008 financial supervision institutions have begun to require from the largest financial organizations development and implementation of effective risk management programs of non-compliance with regulations and standards issued by the supervisory authorities.

Regulation of the Basel Committee on Banking Supervision (2005) draws attention to the results of non-compliance in the form of negative consequences, to which the bank is exposed to when found non-complient with the regulations applicable to its activities. Also the European Directive MiFID informs investment firms, including banks engaged in these activities, about the obligation of appointing a legal compliance supervision unit and the

* Ewa Losiewicz-Dniestrzanska. Tel.: +48 71 3680353; fax: +48 71 3680355.
E-mail address: ewa.losiewicz@ue.wroc.pl

2212-5671 © 2015 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of Academic World Research and Education Center
doi:10.1016/S2212-5671(15)00846-1

necessity to monitor and evaluate its actions. National regulators concerned to emphasize the importance of the individual compliance and compliance functions.

An example from the Polish financial system is a resolution on the Financial Supervision Commission that defined the notion of risk of non-compliance as a result of a bank's failure to comply with legal requirements and recommendations set out by the Polish Bank Association, which indicates the bank's management as the body responsible for compliance with the relevant provisions of the act. Principles of non-compliance risk management are not imposed by regulators either by national or foreign, the way the obligation of risk management are fulfilled by banks depends on the bank's internal solutions. The ISO 16900: 2014 (en) norm presents the assumptions of the Compliance Management System but it is a set of guidelines not ready to use methods and tools. Non-compliance risk management in ISO 16900: 2014 (en) is based on a comprehensive assessment of compliance risk including the monitoring, measurement and analysis.

2. Compliance risk management

The concept of risk can be defined as the product of probability of a potential event and the size of losses that it may generate. The risk of non-compliance of according to Basel Committee is “the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities (compliance laws, rules and standards). (Basel Committee, 2005).

Each institution implementing compliance risk management program, both out of necessity imposed by the regulator as well as from internal needs, develops its own proprietary process based solution tailored to the needs and characteristics of the bank. The compliance risk management process itself in its basic version usually consists of the following stages (Operational Risk Management Policy, 2015; Makowicz, 2011; Risk Management & Compliance Framework, 2014; Risk-based compliance, 2008; ISO 19600: 2014 (en), O'Neill, 2014):

1. Risk identification.
2. Risk measurement.
3. Risk monitoring.
4. Risk control and mitigation.

These stages of compliance risk management process are carried out by compliance units established by a bank (Losiewicz-Dniestrzanska, 2014). Identification of risk applies both to identifying relevant legal obligations by establishing the applicable legal framework and then evaluating its relevance and importance to the business of the bank. This is a very important step for the effectiveness of the further stages of risk management process because the identification of all hazards in the area of non-compliance is determined by the ability to detect real errors in the future. The following factors should be examined (Risk-based compliance, 2008):

- The nature of the risk – what event or incident happens, when and where?
- The source of the risk – what types of people or businesses will be involved?
- The cause of the risk – why does the risk occur, direct and underlying reasons?
- The effect of the risk – what is the impact upon the regulatory outcome, who will be adversely affected?

As a source of identification of risks in the area of compliance banks use all kinds of historical data on violations and penalties imposed on banks, data from operational risk reports and internal audit reports, sentences in consumer lawsuits, whistle-blowing, information from the media, customer complaints and requests, consultancy and projects of domestic and foreign regulators.

The identified potential risk effects should be assessed in respect of their relevance (e.g. classification by importance) in order to differentiate their strength. This will help to measure compliance risk in the next stage of the process, mainly using qualitative tools as with quantitative tools a problem has been found (Birindelli and Ferretti, 2008). Previous experience of banks in risk compliance measurement mainly amounts to developing a risk matrix which determines the amount of risk frequently based on accepted values. An example of a risk assessment will be presented based on the Risk Management & Compliance Framework (2014).

Table 1 illustrates the first step of the risk assessment for potential events by assigning the probability of such an event.

Table 1. Determining the likelihood of the risk occurring.

Rating	%	Likelihood Criteria (within 12-24 months)
1	0-10	Highly unlikely to occur
2	10-25	Possibility of occurrence
3	25-75	Good possibility of occurrence
4	75-90	Likely to occur
5	90-100	Almost certain to occur

The next step to assess the risk associated with the occurrence of a given event is multiplying the impact and likelihood ratings to obtain the risk rating, which is presented in Table 2.

Table 2. Overall risk rating.

		Likelihood				
		1	**2**	**3**	**4**	**5**
Impact	**5**	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

The product: *Impact x Likelihood* gives a result in the form of Overall risk rating set in a range from 1 to 25. Overall risk rating can be aggregated in categories:

1, 2, 3: Minor,
4, 5, 6: Moderate,
8, 9, 10, 12: Significant,
15, 16: Major,
20, 25: Catastrophic.

In Polish banks compliance units do not usually record situations when at the monitoring stage the Overall risk rating is classified in a category above Moderate. The adopted scale is often narrower and consists of 3-2 categories (green, yellow, red) the highest degree of risk during the audit is not reported, the yellow category is a warning and motivates to take corrective actions. The said stage of compliance risk monitoring concerns the detailed review of business activities, transactions, maintain customer accounts, relationships between employees and between employees and customers of the bank (The role of compliance, 2005). At the monitoring stage compliance department cooperates with other units of the bank, e.g. with an audit unit, internal control, risk department (particularly with an operational risk unit), legal department or security department through consultations with these units and using results of their audits and information from their reports.

The last step in the process of compliance risk management - risk control and mitigation aims at reducing the likelihood of causes of errors and their adverse effects. Total elimination of the risk of non-compliance in a bank is not possible, however difficult it is to consider a certain level of risk as acceptable, one has to consider it necessary. Risk at a “zero" level is not possible to achieve, therefore what is left is the necessity to control and reduce the likelihood of errors in the area of compliance and the scope of their negative consequences. Banks use the following control mechanisms that are aimed at reducing risks: internal procedures, staff training, separation of duties, application of the "four eyes" principle, legal opinions, appropriate documentation of transactions, physical security, system mechanisms (access rights, lockouts).

3. Compliance risk monitoring tools in banks

Risk monitoring can be commonly defined as measuring that the risk remains at an acceptable level. The task of

"measuring" in a bank lies within the responsibility of a compliance unit and can be achieved through actions such as the ones below (Certified Global Education, 2015):

- participation in the process of regulation assessment (e.g. new product),
- participation in the process of marketing materials assessment,
- participation in implemented projects,
- participation in meetings of the bank's Audit Committee,
- participation in risk assessment in individual units (meetings with the bank's business units, periodical reports, verification of policy imposed control functions implementation),
- participation in the process of dealing with complaints of bank customers,
- support tools (AML, conflicts of interest, own transactions, record of benefits),
- training (personal data protection, ethics, bank secrecy, AML).

These activities support the monitoring of compliance risk, which is done using qualitative and quantitative tools. Qualitative tools primarily include risk maps that by visualizing business processes in a bank show the relationship between them and the reasons for any errors in the implementation process (Patchin and Carey, 2012).

Another example of risk maps are heat maps which quickly focus on areas that require immediate and precise attention. An example of a heat map is the risk chart in Section 1 of Article (table 2. Overall risk rating):

- The second group of tools for monitoring compliance risks are quantitative tools, however financial institutions pay attention to the following critical points when trying to assess the risk (Birindelli and Ferretti, 2008) difficulty in quantifying the risk impact.
- shortage of internal and, above all, external loss data (particularly useful when the risk originates from events “Low Frequency-High Impact”).
- the “history” of losses is not very indicative.

Quantitative tools in compliance risk monitoring are mainly based on indicators that are characterized by abundance, easy accessibility, ease of determining thresholds / reference points on the basis of historical data, or with respect to the parameter set by the regulator. As examples from the compliance range the following indicators can be given (Are, 2013; Kroll, 2012):

- the number of non-compliance identified by test monitoring,
- the number and status of recommendations of the compliance unit,
- the number of violations,
- the number of calls to the bank hotline having the nature of the complaint,
- the number of analysed and reported suspicions of money laundering,
- the measurement of the costs incurred in the implementation of new regulations,
- the number of customer complaints,
- the number of customer complaints to regulators,
- the number of cases at regulators,
- the number and value of claims paid,
- the number and value of the penalties imposed by regulators,
- legal process and lawsuits costs resulting from non-compliance,
- the number of investigations conducted,
- feedback from worker surveys in the field of ethics (whistle-blowing),
- delay in registration of transactions above the applicable amount,
- the number of own transactions in violation of the rules of investment,
- the number of overdue corrective action.

Monitoring is a control mechanism for certifying compliance with the requirements of the current processes, but it should be a planned, regular, action based on risk evaluation with correction measures of identified errors.

Features of indicators, despite their quantitative nature, do not measure risk and show only the current trend with reference to the historical background and in relation to the adopted thresholds. In compliance risk monitoring data collected is used in banks in large databases, tailored to the specificities of the bank (Wehmeyer, 2005). This

properly selected data is used to develop an early warning system about a possible increase in risk. Due to the repetitive control measures for monitoring business processes (including banks), it is recommended to use IT tools.

An example of a comprehensive modelling and analysis process improvement tools is business process management system – ADONIS1[1]. This system will be used in the article in order to develop a complaint process model using indicators signalling the level of claims realized in bank X that in the aspect of risk monitoring compliance are of high importance.

Transactions finalized with the use of bank cards have a rather large and non-decreasing number of disputes between banks and their customers, so as an example of complaint process model we will use for the problem of the complaint with regards to an ATM cash withdrawal.

During the operation of ATM cash withdrawal there may be some irregularities, e.g. the customer may not receive the amount of money desired or may not receive cash at all. Such situations are causes of customer complaints.

The applied tool gives the possibility to enrich the basic business process model with indicators signalling process phases at different stages of its implementation. The tool has been equipped with two classes of modelling on indicator processes realization: "index" which will refer to a particular process or activity, and "indicator review" which will collect all the indicators of the model and makes it possible to initiate and update the values assigned to the indicators.

Indicators defined in the model function based on planned and ongoing values. These values can be manually entered into the system, can be downloaded from MS EXCEL spreadsheets or databases using the classic SELECT statement. The ADONIS system automatically after importing data signalizes the status of the indicator in the process model (in graphical or tabular), indicating the level of the scope of the results achieved. This is done by determining the performance characteristics of the indicator defining its behaviour, which may look like this:

- the current value < planned value + 5% - green indicator,
- the planned +5% <= the current value < planned value +15% - yellow indicator,
- the current value > = planned value +15% - red indicator.

The example is a proposal to develop a method for early warning against adverse changes that occur in the process of bank customer complaints. It can form the basis for development of the application to other areas of bank operations.

Many of the indicators used in compliance risk monitoring is also utilised to monitor the use of operational risk. Both of these units have a number of common areas, which inspires the banks to seek effective solutions and propagates the need for integration of operational risk with the risk of non-compliance (Let's, 2013).

4. Operational risk and compliance risk

In some organizations, including banks, compliance units are not independent but are often subject to the legal department due to the proximity to law regulating. This solution is not beneficial for the individual compliance due to the domination of its position in the organization by the legal issues. Connecting compliance units with the legal department will focus on the procedures, internal rules and criminal sanctions, and not on the detection and prevention of threats.

Another approach that has become increasingly popular because of the close relationship between compliance risks and operational risks is the integration of compliance units with operational risk unit. One of the arguments of such a solution is the quantitative approach to risk management (compliance and operational) as both of the units utilize a common set of indicators. In the area of compliance the values of key indicators are calculated in the area of operational risk, whereas the information about significant violations is transmitted from the compliance to operational risk area. The benefits of the combination of units primarily include the independence of the operational risk unit across the bank's organizational structure, ownership of control capacity, which will also benefit the

[1] http://www.boc-eu.com

compliance unit. This solution, however, carries the risk that the non-compliance management activities can be dominated by the tasks of operational risk management.

The best solution that gives the greatest self-reliance and independence of the compliance unit is its independence. The big advantage of this solution is the subordination of the unit directly to management board and the audit committee but at the expense of direct access to legal knowledge on non-compliance risk and the knowledge of the specificities of the business.

5. Conclusions

The article highlighted the growing role of compliance units and compliance risk management. Monitoring compliance risk is a very important aspect in the process of compliance risk management. The article pointed out the difficulty in measuring compliance risks which relate mainly to quantitative techniques, based on the conventionally accepted values, as in the case of reference values for indicators.

The large number of indicators used in the compliance management and their variety may become a nuisance when it comes to utilizing them, which ultimately may result in abandoning them altogether. A good solution to prevent this is to support the compliance risk monitoring with an IT software tool with built-in warning system, which is provided by BPMS -ADONIS.

The quantitative nature of indicators in the area of compliance risk monitoring and partial duplication of the indicators in the area of operational risk may suggest integration of these areas. This article attempts to demonstrate that it is preferable to keep the compliance units independent while maintaining close cooperation with the area of operational risk and other areas of the bank.

References

Are companies using the right metrics to measure compliance risk? Risk&Compliance Journal. From the Wall Street Journal. September 4, 2013. Available from: http://deloitte.wsj.com/riskandcompliance/2013/09/04/are-companies-using-the-right-metrics-to-measure-compliance-risk/

Birindelli, G., Ferretti, P., (2008). Compliance risk in Italian banks: the results of a survey. *Journal of Financial Regulation and Compliance* 16 (4), 335-351.

Certified Global Education, 2015. Internal training materials, Warsaw.

Commission Directive 2006/73/EC implementing Directive 2004/39/EC.

Compliance and the compliance function in banks, 2005. Basel Committee on Banking Supervision, Bank for International Settlements.

ISO 19600:2014(en), Compliance management systems — Guidelines.

Kroll, K., (2012). Measuring the Effectiveness of Compliance. Complianceweek, April 2012. Available from: http://www.pwc.com/en_US/us/risk-assurance-services/assets/pwc-cw-measuring-effectiveness-of-compliance-kipp.pdf

Let's make a difference: Managing compliance and operational risk in the new environment, 2013. PWC FS Viewpoint, August 2013. Available from: www.pwc.com/fsi

Losiewicz-Dniestrzanska, E., (2014). Ryzyko braku zgodnosci w banku (Non-compliance risk in the bank), Annales UMCS, Sectio H Oeconomia, 107-116.

Makowicz, B., (2011). Compliance w przedsiębiorstwie (Compliance in the enterprise). Oficyna a Wolters Kluwer business, Warsaw.

MiFID - Markets in Financial Instruments Directive (Directive 2004/39/EC).

O'Neill, A., (2014). An action framework for compliance and governance, *Clinical Governance*: *An International Journal* 19 (4), 342-359.

Operational Risk Management Policy, 2015. Black Sea Trade &Development Bank. Available from: http://www.bstdb.org/about-us/ key-documents/Operational_Risk_Management_policy.pdf

Patchin, C., Carey, M., (2012). Risk assessment in practice. Deloitte & Touche LLP, Available from: https://www2.deloitte.com/content/dam/Deloitte/ global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf

Risk –based compliance, 2008, Available from: www.betterregulation.nsw.gov.au

Risk Management & Compliance Framework, 2014, Available from: http://www.canterbury.ac.nz/ucpolicy/ GetPolicy.aspx? file=Risk-Management-And-Compliance-Framework.pdf

The role of compliance, 2005. Securities Industry Association, white paper. Available from: http://www.sifma.org/uploadedfiles/societies/sifma_compliance_and_legal_society/role_of_compliance_white_paper%20%282%29.pdf).

Wehmeyer, K., (2005). Aligning IT and marketing – the impact of database and CRM, *Journal of Database Marketing & Customer Strategy Management* 12, April 2005, 243-256.