Culegere de articole selective ale Conferinţei Ştiinţifice Internaţionale „Competitivitatea şi Inovarea în Economia Cunoaşterii”, 22-23 septembrie 2017, Chişinău, Vol. III
E-ISBN 978-9975-75-897-0

DEVELOPMENT OF INTEGRATED FRAMEWORK FOR INTERNAL CONTROL OF INFORMATIONAL SYSTEM IN THE BANKS OF REPUBLIC OF MOLDOVA

Ph.D., Assoc. Prof., Stela CIOBU

Academy of Economic Studies of Moldova, Bănulescu-Bodoni 61, str. Chisinau, Republic of Moldova, MD-2005, + 373 22 40-27-09, www.ase.md

Abstract

The internal audit of IT from banks of the Republic of Moldova has to follow a more holistic view and focus its progress on the following priority areas: challenge management and policy; to establish and evaluate risk tolerance, determine governance and strategic objectives. The aim of the present article is to identify a modern integrated mechanism to establish a favorable dialogue between the internal audit of IT and risk management within the banks of the Republic of Moldova.

Key words: *informational system, internal control, bank risks management, IT governance, control environment, risk assessment, Risk Based Internal Auditing.*

JEL CLASSIFICATION*:* G14,G21, O32.

Increasing economic pressures are pushing the banking community to increase the effectiveness of risk mitigation efforts and focus on a more holistic approach to risk management. Consequently, the internal audit function plays a crucial role in the ongoing maintenance and assessment of a bank’s internal control, risk management and governance systems and processes – areas in which supervisory authorities have a keen interest**.** Given the banking supervisory review process, from a bank’s audit perspective, obviously it is of a primary importance to focus on internal risk management capabilities via internal control reviews of residual risks relative to the risk “appetite” of the bank. Therefore, as the banks are required to adopt risk management system in all areas of their activity, a supervisor also looks up to the systems and practice of banks in assessing, managing and controlling risks. This has led to the need for adoption of Risk Based Supervisory (RBS), wherein the supervisory resources will be directed towards the areas of greater risk to the supervisory objectives which aim at protecting the interest of depositors, stability of the banking system and development of banks as agents of economic growth. Under the RBS approach, the banking internal auditing tends to a risk-based approach as to synchronize the supervisory requirements.

The Institute of Internal Auditors (IIA) defines the Risk Based Internal Auditing (RBIA) as a methodology that links internal auditing to an organization's overall risk management framework. RBIA allows internal audit to provide assurance to the board that risk management processes are managing risks effectively, in relation to the risk appetite.

The focus of the RBIA is on the risk identification, prioritization of audit areas and allocation of audit resources in accordance with the risk assessment. As the name suggests, the fundamental principle of process based auditing is the analysis of complex processes and systems rather than individual transactions or process parts – considering the case of consumer credits area, all the steps involved in the process of granting, approval, drawing and repayments or collections and recovery are analyzed throughout the entire bank, not only in relation to one branch (if the sample of cases from one branch is used during the testing, the conclusions are then generalized and applied on the entire bank). The risk-based approach includes formal annual planning, updating the plan before audit segments begin, and periodic feedback from management and the audit committee regarding report content expectations. The audit scope is adjusted based on all of these factors and gives the internal auditor a keen ability to understand and react quickly to management and audit committee concerns regarding risk and audit coverage. A professional internal audit activity can

E-ISBN 978-9975-75-897-0

best achieve its mission as a foundation of governance by positioning its work in the context of the bank's own risk management framework. In the Republic of Moldova, the audit function, within the banking sub-sector, has not been fully taped. This could be seen in the numerous cases of errors, intent to defraud and other fraudulent acts recorded in the banking industry. It is therefore, no wonder that the distress in the banking sub-sector in the nineties reflected lack of effective control mechanism of the audit function in the banking industry. The experience of failed banks in Moldova calls for reinforcement of internal audit procedures in order to strengthen the control system in the banks from the Republic of Moldova. Moreover, the weak regulatory framework in regard to the bank's internal audit function proves the incipient phase in the internal audit evolution and acquired capacities. Exception make some of banks totally foreign owned, as the subsequent entry in the banking sector of the Republic of Moldova of financial groups with European reputation mainstream their efficient risk assessment and management internal systems.

Domestic banks, in their efforts to comply with the multiregulations, should realize that complying with all the mandatory regulations is too cumbersome, because many times the data and approach have to meet different requirements that are quite similar, resulting in duplicated efforts and increased costs. Banks from the Republic of Moldova have to intensify its efforts to adapt to the Enterprise Risk Management Framework (ERM) released by COSO (Committee of Sponsoring Organizations of the Tread way Commission) as a framework to drive their initiatives in risk management beyond Basel norms and regulatory compliances.

In September 2004, COSO (2004) issued the Enterprise Risk Management Integrated Framework that provides a model of the ERM process and defines ERM as: process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

COSO has established a common internal control framework against which companies and financial organizations may assess their control systems. The COSO framework is based on the following key concepts:

– internal control is a *process*. It is a means to an end, not an end in itself;

– internal control is affected by *people*. It is not merely policy, manuals, and forms, but people at every level of an organization.

– internal control can be expected to provide only *reasonable assurance*, not absolute assurance, to an entity's management and board;

– internal control is geared to the achievement of *objectives* in one or more separate but overlapping categories.

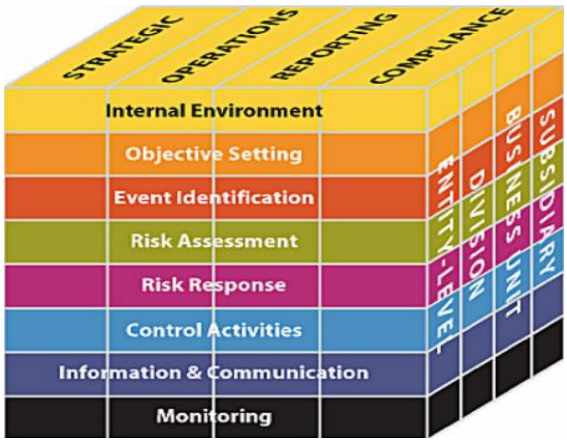

Figure 1. COSO Framework.

Source: ***http://www.bussvc.wisc.edu/intcntrls/cosoframework.html.***

E-ISBN 978-9975-75-897-0

Table 1. Principles for effective internal control (by COSO)

Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies suitable objectives 7. Identify analyses risk 8. Assesses fraud risk 9. Identifies and analyses significant change
Control activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys though policies and procedures
Information and Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and / or separate evaluations 17. Evaluates and communicates deficiencies

Source: http://www.bussvc.wisc.edu/intcntrls/cosoframework.html.

The COSO ERM framework has all the components that could help domestic banks to stand a chance to derive business value while meeting compliance requirements. The ERM Framework is structured around eight key components and four key objectives of business: strategic, operations, reporting and compliance. One of the issues surrounding ERM is the role internal auditors should acquire in ERM processes. Because internal audit professional standards take a risk based approach, the internal audit function has to extend a significant interest in the enterprise’s risk management process, as it affects internal audit’s professional responsibilities.

Despite internal audit’s natural interest in ERM, there arises a debate as to the role of the internal audit function in ERM. To establish a risk management framework with internal auditing participation in the system, run it effectively, and audit the effectiveness and maturity level of bank’s risk management, the worldwide accepted integrated approach should have a leading or consulting role in banks of the Republic of Moldova. Auditing approaches are generally acquiring the name of the auditing focus point. The focus point in auditing is defined as “control focused auditing” on which controls are applied. Following the change, the sliding of focus point towards risks, the publishing of the Enterprise Risk Management Framework by COSO in 2004 and the efforts for completing the internal auditing to risk management process have contributed to the emergence of the ERM Based Internal Auditing.

ERM Based Internal Auditing is a kind of auditing approach based on determining and evaluating the banks’ risk characteristics. It designs the proper auditing process and procedures which suits to the institution risk range, in line with risk matrix or risk map and are based on the proper distribution of limited auditing sources to risk evaluation. ERM Based Internal Auditing aims at increasing the efficiency and auditing the effectiveness of risk management system. The internal auditing unit following this approach runs the services of trust and consulting for the purpose of risk management activities. The ERM Based Internal Auditing, manipulated by enterprise risk management principles, and compared to the traditional auditing functions, determines whether the enterprise risk management in the bank can manage the risks, in general, in accordance with the approved limits of the risk acceptance and risk appetite. After auditing activities, through comparison between the current situation and desired situation determined through the risk management process, it is aimed to eliminate the defaults of the risk management system.

E-ISBN 978-9975-75-897-0

Table 2. Components of and internal control framework

Control Environment	commitment of leadership and senior management to effective internal control, adhere to high ethical standards, oversight by those in governance, and support of competent employees.
Risk Assessment	- dynamic and iterative process for identifying and analyzing risks towards achieving the organization's objectives; - forms the basis for determining how risks should be managed; - identifies the areas where the greatest threat or risk of inaccuracies or loss exist, with the greatest risk receiving , the greatest attention and control; - consideration given to dollar amounts, nature of transactions and impact on organizational reputation.
Control Activities	actions established by policies and procedures to help ensure management directives to mitigate risks to the achievement of objectives are carried out at all levels of the organization, at various stages of operating processes and over the technology environment.
Information and Communication	- information generated at operational level and communicated across and up the organization to enhance decision – making; - policies and procedures communicated downward through the organization to support internal control functions; - information and communication to be fully integrated with the other components of the framework and includes communication with outside parties about internal control accountability
Monitoring and review	- applies to all five components of internal control; - should fit the organization; - takes on increased importance as the organization recognizes the need for timely and effective monitoring that provides feedback on the operation of the other components, and extends beyond financial reporting to compliance and operations.

Source: http://www.bussvc.wisc.edu/intcntrls/cosoframework.html.

Among ERM units, the control environment targeting, event risk defining, risk evaluating and risk behavior are overlapping with understanding the bank’s structure for auditing and planning the auditing. While the control activities, the sixth component of ERM, is in-line with carrying out auditing activities, the information and communication and the observation process are parallel with process of reporting in internal auditing.

The stages of ERM based internal auditing are arranged as evaluating the risk quality, planning the auditing within the frame of auditing strategy, creating individual auditing task and reporting the auditing. Evaluating the risk management quality and risk recording are their direct connection points with risk management process. Also, the risk register and auditing universe are supported by the data of risk management system through risk recording.

The internal audit procedures focused on ERM principles would help banks from the Republic of Moldova to step out from the “silo” approach to risk management (i.e. different internal groups responsible for each type of risk) and move towards the holistic view of enterprise wide risks. ERM can help the domestic banks to eliminate the duplicates and, redundancies in risks and related control procedures that exist mainly because different groups define same risk differently, implement different control procedures and use different analytical models based on different assumptions and underlying data sets.

Successful financial institutes understand the benefits of information technology (IT) and use this knowledge to drive their shareholders' value. They recognize the critical dependence of

E-ISBN 978-9975-75-897-0

many business processes on IT, the need to comply with increasing regulatory compliance demands and the benefits of managing risk effectively.

COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout financial organizations. COBIT emphasizes regulatory compliance, helps organizations to increase the value attained from IT, enables alignment and simplifies implementation of the enterprises' IT governance and control framework.

COBIT was initially "Control Objectives for Information and Related Technologies," though before the release of the framework people talked of "CobiT" as "Control Objectives for IT" or "Control Objectives for Information and Related Technology." The framework defines a set of generic processes for the management of IT, with each process defined together with process inputs and outputs, key process-activities, process objectives, performance measures and an elementary maturity model. COBIT also provides a set of recommended best practices for governance and control process of information systems and technology with the essence of aligning IT with business.

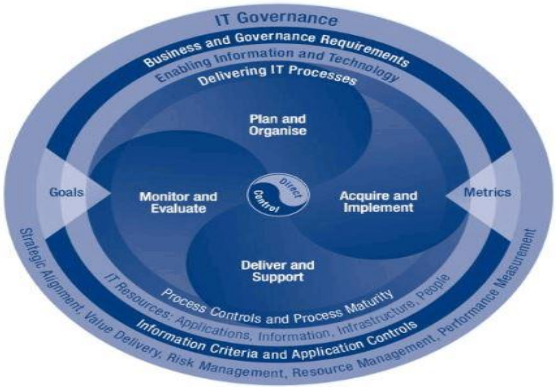

Figure2. COBIT framework.

Source:.https://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx.

If a risk is the potential that something bad can happen, then a control objective ensures that the risk does not materialize. Looking at control objectives this way quickly enables you to get a catalog of potential risks to refer to when you are looking for items to consider in your risk assessment. This risk list can subsequently be used to define audit programs that are comprehensive and to ensure that the organization, through your audit and assessment of controls, meet their objectives. There are many interesting and unique risks to consider when you are planning an audit and assessing the risks of an IT process or system. Once identified, risks are considered to be applicable to the process or system that is the object of your audit scope. You must prioritize these risks in order to maximize your effort in reviewing how they are controlled.

Figure 3. IT Governance focus area.

Sources:https://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT-4.1-Brochure.pdf.

E-ISBN 978-9975-75-897-0

Strategic alignment - focuses on ensuring the linkage of business and IT plans, on defining, maintaining and validating the IT value proposition, and on aligning IT operations with enterprise operations.

Value delivery - is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.

Resource management - is about the optimal investment in, and the proper management of, critical IT resources: processes, people, applications, infrastructure and information. Key issues relate to the optimization of knowledge and infrastructure.

Risk management - requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, transparency about the significant *risks to the enterprise, and embedding of risk management responsibilities into the organization.*

Performance measurement - tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

CobiT is very versatile and was created from an extensive source list that is both comprehensive and authoritative. It was designed with the business processes and objectives in mind so it would fit naturally into any existing IT environment. It is broken down in several layers of detail so the needs of the various levels of management and oversight requirements can all be best met.

IN CONCLUION, the internal audit of IT from banks of the Republic of Moldova has to follow a more holistic view and focus its progress on the following priority areas:

a) challenge management and policy: challenge management to adopt appropriate policies and procedures as well as effective controls; challenge the effectiveness of policies that are outdated, ineffective, or not up to current industry or regulatory standards;

b) establish and evaluate risk tolerance: understand risks the institution faces, and confirm that the board of directors and senior management are actively involved in setting and monitoring compliance within the institution's risk tolerance limits; evaluate the reasonableness of established limits, and perform sufficient testing to make sure that management is operating within these limits and other restrictions;

c) determine governance and strategic objectives: evaluate governance at all management levels within the institution and within all significant business lines; evaluate the adequacy and effectiveness of controls to respond to risks within the organization's governance, operations, and information systems. Communicate any concerns to the board of directors and senior management.

Particularly, to establish a favorable dialogue between the internal audit of IT and risk management within the banks of the Republic of Moldova, the modernization efforts should be concentrated on:

- extending the implementation of RBIA;
- developing the audit methodology around the top-down COSO process of ERM framework (COSO II Model);
- implementing automated audit procedures targeting acquiring capacity for a Continuous Auditing of IT.

The banks of the Republic of Moldova will need to place greater emphasis on developing an integrated view of risk across all the risk types and the internal audit objective should encompass a more advanced integrated approach on the banking risks as well. For a responsive or progressive internal audit, domestic banks should ensure that the risk management framework is an integral part of the audit planning methodology. Systems to monitor and review risks and the risk management process require careful selection, targeting and planning as they absorb scarce resources.

E-ISBN 978-9975-75-897-0

BIBLIOGRAPHY*:*

1. NASTASE, P.; CAIA, F. Study regarding information systems audit for e-business. Audit financiar, 2015, nr. 3.
2. RUPPERT, Mark P. Roles and Responsibilities – Corporate Compliance and Internal Audit, CPA, CIA, CISA, CHFP.
3. HUNTON, J.; BRYANT, S.; BAGRANOFF, N. Core Concepts of Information Technology Auditing, John Wiley & Sons, 2004.
4. IT Governance Institute, Board Briefing on IT governance, 2nd Edition, ITGI, 2003.