MODEL FOR IT GOVERNANCE ASSESSMENT IN BANKS BASED ON INTEGRATION OF CONTROL FUNCTIONS

Ivana Dvorski Lacković
PBZ stambena štedionica d.d., Croatia
ivana.dvorski-lackovic@pbz.hr

Abstract:
Nowadays banks are struggling with risky environment and constant technological changes in order to achieve best possible results. Information technology is crucial for banks to be able to create, implement and deliver new services and products but at the same time it is source of significant risks. In order to achieve results that are sustainable in long term banks need to assure adequate IT governance. Regulators give guidelines and frameworks for IT governance but very often bank managers and supervisors find themselves confused by actual assessment of their IT governance. This paper proposes a new model for IT governance assessment in banks that is based in integration of control functions. Basis for model development is identification of IT audit areas that are then analyzed by IT risk and IT compliance components. Model enables banks to assess their IT governance and prioritize IT areas that need improvement what in the end can lead to increase in banks effectiveness and results.

Keywords: IT Governance, management, assessment, control functions, banks

1. INTRODUCTION

Due to the ongoing financial crisis regulators, academic public and banking experts are becoming more aware of risks of contemporary business activities and importance of managing information technology (further in text: IT) in line with good practices of corporate governance. Banks are nowadays fully dependent on IT. On one hand IT enables banks to create, implement and offer clients new services and products and on the other IT is source of very significant risks for banks. According to Basel Committee IT risks are classified as subcategory of operational risk. According to widely accepted definition of Bank for International Settlements operational risk is the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events (Sound practices for the Management and Supervision of Operational risk, BIS, 2003). Due to constant and rapid technology changes regulators are putting accent on significance of operational risk management, its proper supervision and relevance for corporate governance.

IT governance as subcategory of corporate governance has its specificities and is of crucial importance for banks in order to keep performing their business activities by minimizing risks and accomplishing their full potential, but bank managing and supervising boards often remain unsecure how to assess their IT governance, effects it has on bank and areas that need improvement. Aim of this paper is proposition of model for IT governance assessment in banks that is based on integration of control functions. Author will do this in three steps:

1) systematization of existing frameworks and knowledge on IT governance in banking industry,
2) explanation of need for integration of control functions for model development,
3) definition of model and its components.

2. WHAT IS IT GOVERNANCE?

Requirements of Basel II and Basel III related to information systems are related to accentuation of importance of IT risk as a part of operational risk system and significance of IT corporate governance implementation but taking into account that it is impossible to establish fixed rules due to quick technology changes and individual differences between banks. Basel documents are also very focused on reliability of information system in part related to information system safety and its accessibility. Therefore individual banks have freedom to choose measures which they are going to implement in everyday business activities with the aim of improving their IT governance and reducing IT risk. According to document ISO/IEC 17799 IT governance is integral part of organizational management and responsibility of managing and supervising boards and it consists of leadership, organizational structure and processes that ensure IT is used as enhancer of organizational strategy and goals. IT governance implies that IT processes are fully integrated into life cycle of business process and it influences on quality of service and business agility (Spremić, 2009, pp. 906). Van Grembergen and De Haes (2005) defined IT Governance as the organizational capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT. The primary focus of IT governance is on the responsibility of the board and executive management to control formulation and the implementation of IT strategy, to ensure the alignment of IT and business, to identify metrics for measuring business value of IT and to manage IT risks in an effective way.

According to Peppard and Ward (2004) IT is nowadays used as business transformer and factor that can increase organizational value. Different authors have tried to identify and quantify elements of adequate IT governance. Weill and Ross (2004) allege that structure of decision making process, process compliance and access to communication are key elements. Sohal and Fitzpatrick (2002) notice that IT steering committee, centralization of IT decision making process and inclusion of higher level management in decisions regarding IT brings success to IT governance, but this research was not empirically confirmed. Vaswani (2002) confirms positive relation between IT governance and existence of IT steering committee, inclusion of higher level management in decisions regarding IT and performance measurement system. Filatochev (2007) believes that control and supervisory functions are crucial in order for higher managers to be able to minimize risk (aspect of value preservation) and free managerial potential of IT (aspect of value creation). Research shows that compliance culture and ethics in business related to IT are crucial in implementation of IT governance (Ali, Green, Parent, 2009).

3. CONTROL FUNCTIONS IN BANKS AND THEIR INTERCONNECTION IN IT AREA

Basel documents define three obligatory control functions in banks: risk control, compliance and internal audit. Risk control function is responsible for risk analysis, risk monitoring, reporting and participation in the design, implementation and oversight of risk management models and models. Compliance is in charge for identification and assessment of compliance risk, advising management board on implementation of relevant laws, standards and rules, assessing effects that changes in relevant regulations will have on the operation of a bank, verifying compliance of new products or procedures with relevant laws and regulations as well as amendments to regulations and providing advice as regards the preparation of training programs related to compliance. Internal audit is in charge of examination and evaluation of wholesome business processes and control mechanisms. Each of these control functions is applicable on IT, i.e. we can discuss IT risk control IT compliance and IT audit.

What do these control functions have in common and what are their differences?

All three control functions are fully independent organizational units and are responsible to management board. Their purpose is insurance of banks appropriate business activity performance, i.e. maximizing profit and at the same time minimizing risk and being compliant with external and internal acts. Also compliance is sometimes seen as part of wider enterprise risk management system. In banking practice and risk systematization the risk of not being compliant is part of operational risk. This means that there is space for integration of these functions in order to achieve synergetic effects on governance. This integration is of course partial and relates to parts of functions that are logical to integrate while in other parts functions remain independent. Internal audit is different from previous two functions in sense that besides other business areas it audits, one of its audit areas are control functions (risk and compliance). Regarding IT internal audit every national regulator defines key IT areas that internal audit needs to examine and evaluate.

4. MODEL FOR IT GOVERNANCE ASSESSMENT

Basic idea of this paper is to present a new model for assessment of IT governance. Having in mind that effective IT Governance influences overall business performance it is of crucial importance for organizations to have valid model that enables them adequate, objective and detailed assessment of its IT governance. This model is based on premise that control functions that operate within banks can integrate for purpose of assessing IT Governance and contribute its improvement. Regulator (Basel Committee, Bank for International Settlements) defines three obligatory control functions that need to operate within banks: risk control function, compliance function and internal audit. To authors knowledge so far there has been no research on how all three control functions (risk, compliance and internal audit) can be integrated in order to assess IT governance.

Starting point when defining model are previously mentioned key areas that every national regulator defines for regular IT internal audits. This model is done based on legislative proscribed by Croatian National Bank and according to it IT Audit component consists of 18 regulatory areas.

1) Management of information and IS safety
2) IT risk management
3) Physical and logical access control management
4) IS asset management
5) Operational and system files management
6) Backup management
7) Service provider management
8) Assets suppliers management
9) IS development management
10) Physical safety management
11) Password management
12) Configuration management
13) Change management
14) Business continuity management
15) Disaster recovery

16) Incidents management
17) Malicious code protection
18) Application of internal acts regarding IS

Integration of control functions is done in way that each of these 18 areas is analyzed through its IT risk and IT compliance component. The IT Risk component consists of:

1) Analysis of operational losses is historical component; for every regulatory area is estimated representativeness of operational losses.
2) Scenario analysis is a forward-looking concept; for every regulatory area is estimated impact in terms of frequency and potential loss in case of operational loss event related to this regulatory area occurs.
3) Reputational risk is assessed for each regulatory area in terms of income reduction in case of operational loss event occurrence.

The IT Compliance component consists of:

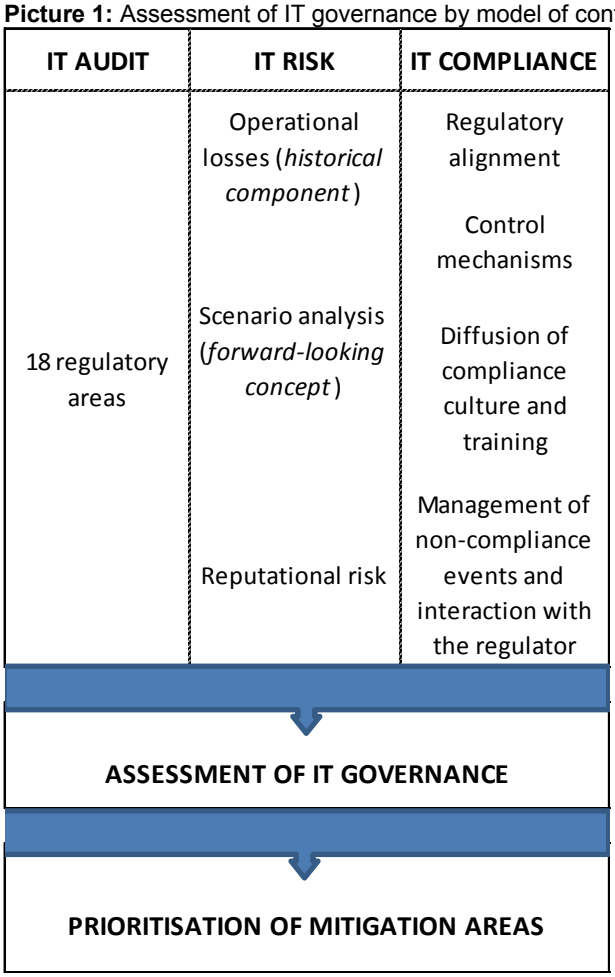
1) Regulatory alignment is related to existence of continuous alignment between external regulations and internal policies and to coverage of the requirements set in regulations with internal policies.
2) Control mechanisms relate to definition and formalization of controls, effective performance of controls by the responsible units, adequacy of the resources assigned to control activities and adequacy of the controls outcomes diffusion.
3) Diffusion of compliance culture and training relates to diffusion on knowledge on external regulation and internal acts regarding certain regulatory area organization wide and efficiency of internal training regarding compliance external and internal acts related to regulatory area.
4) Management of non-compliance events and interaction with regulator is related to definition of processes and procedures regarding compliance of non-compliance events, involvement of institutions employees in new regulations assessment before they are being launched and effective interaction with national regulators.

Each component of model is given a numerical value, i.e. model is quantified. Model quantification enables delivery of following results:

- evaluation of IT Governance by ranking 18 IT regulatory areas according to their governance potential,
- prioritization of IT areas whose governance needs to be improved.

Model is shown in Picture 1.

Picture 1: Assessment of IT governance by model of control functions integration



Source: author's picture

5. CONCLUSION

In this paper author gave proposition of a new model of IT governance assessment in banks. Model is based on integration of three control functions. Model enables banks to get more insight into their IT governance by analyzing every area of obligatory IT internal audits by two perspectives: IT risk and IT compliance. IT risk analysis is based on both historical and forward-looking concept and it includes assessment of reputational risk. IT compliance analysis includes regulatory alignment, control mechanisms, diffusion of compliance culture and training and management of non-compliance events and interaction with the regulator. Taking into account all these three control function perspectives bank gets a companywide oversight over its IT governance, processes behind it and areas that need improvement. It is expected that by assessing IT governance by this model and prioritizing key areas for action banks can achieve sustainable long term growth and profit and minimization of risks which means that bank is behaving both financially and socially responsible towards its clients, employees and stakeholders.

REFERENCE LIST

1. Ali, S., Green. P., Parent, M. (2009). The Role of a Culture of Compliance in Information Technology Governance, *Proceedings of the 2nd International Workshop on Governance, Risk and Compliance (GRCIS'09)*. Amsterdam.
2. Filatotchev, I. (2007). Corporate Governance and the Firms Dynamics: Contingencies and Complementarities. *Journal of Management Studies*, *44*(6), 1041-1056.
3. ISO/IEC 17999:2005 Information Technology – Security techniques – Code of practice for information security management
4. Peppard, J., Ward, J. (2004). Beyond strategic information systems: towards an IS capability, *Journal of Strategic Information Systems*, *13,* 167-194.

5. Sohal A., Fitzpatrick P. (2002). IT Governance and Management in Large Australian Organizations, *International Journal of Production Economics, 75*(1), 97-112.
6. Sound practices for the Management and Supervision of Operational risk, Basel Committee Publications, *96*.
7. Spremić, M. (2009). IT Governance Mechanisms in Managing IT Business Value, *WSEAS Transactions on Information Science and Applications*, *6*(6), 906-915.
8. Van Grembergen, W., De Haes, S., (2005). Measuring and Improving IT Governance Through the Balanced Scorecard, *Information System Control Journal*, *2*.
9. Vaswani, R. (2002). IT Governance and management in Australian large companies, *International Journal of Production Economics, 75*(1), 97-112.
10. Weill, P., Ross, J. W. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Boston, Massachusetts: Harvard Business School Press.