IT governance and information system auditing practice in credit institutions in the Republic of Croatia

Mario Spremic, Marijana Ivanov, Bozidar Jakovic

***Abstract*—** Main objective of this paper was to stress the necessity for measuring the level of various risks the companies are exposed to in financial sector. We particularly focused on methods and frameworks for measuring and managing the level of operational risks in credit institutions. It can be done by conducting regular information system audits (IS audits). Information system audit represents a wide range of audit, managerial, analytical and technological activities with the main objective of thoroughly reviewing the effectiveness of control procedures in various parts of IS, conducting analytical tests and collecting evidences which helps in evaluating the level of operational risks and measuring the maturity level of IS. IS auditing is conducting according to various internationally accepted methodologies (such as CobiT), industry based best practices and/or framework (such as Basel III, PCI DSS or similar) or national and transnational regulation provisions. External (CobiT methodology) and especially national regulation framework for conducting IS audits in the Republic of Croatia are explained and analyzed in further details. Also, the methodology for conducting IS auditing is presented and maturity levels explained (5 point scale system with a qualitative marks which range from completely unsatisfactory to completely satisfactory). In the paper we describe the continuous quality control system which enables national regulatory body (Croatian National Bank) to control the quality of IS audits report. The results of assessing the level of operational risks in credit institutions in the Republic of Croatia which arises from external IS auditing activities in 2010 were depicted (11 credit institutions satisfactory manage the level of operational risk, 18 partially satisfactory and 2 partially unsatisfactory). Upon the long-lasting (3 years) in-depth case study analysis, we investigate in further details if the practice of managing operational risks in a small credit institution is improving by conducting regular IS audits and obeying to regulatory framework.

***Keywords*—** CobiT, Information System Audit, Operational Risk

I. Introduction

In recent years it became apparent that, if not managed properly, operational risks can make serious negative impact on businesses in financial sector. The operational risk includes the risk of losses resulting from inadequate internal processes including inadequate information system and supported technology in conducting business transactions. For example, any disruption of conducting financial transactions can have direct (losses in revenues) and indirect (reputation risk) negative impact on organizations. In this paper we stressed the importance of managing the operational risks in credit institutions by conducting regular information system (IS) audits. Information system audit (IS audit) represents a wide range of audit, managerial, analytical and technological activities with the main objective of thoroughly reviewing the effectiveness of control procedures in various parts of IS, conducting analytical tests and collecting evidences which helps in evaluating the level of operational risks and, finally, recommending company's Board's the corrective counter-measures to lower the unacceptable operational risks [15].

As financial transactions are conducted by support of modern information technology (IT) and information systems (IS), it is clear that risks associated with their usage can't any more be treated as 'technical' (low level) risks, but as 'business' (strategic risks) which needs holistic managerial approach. Gartner [5] stands on that point that IT related risks (operational risks) should be treated as business (strategic) risks and that IT Governance (or rather continuous control monitoring) procedures should be in place to effectively manage it. They reports that operational risk acceptance more-properly belongs with the business "owners" of the information assets and business processes. Beyond the realm of IT, it's relatively well-understood that business managers "own" their processes and are accountable for the associated risks and controls.

IT Governance as a relatively new concept introduced in the late 1990s, has gained importance in the 21st century due to well-known collapses (Enron Inc, WorldCom, Parmalat, etc.) and the need for a better reporting and financial disclosure system [12]. International and national regulatory provisions (for example, Sarbanes-Oxley act) helped in understanding control mechanisms in modern IS/IT environment and resulted in further impetus for IT Governance issues world-wide [12]. While enterprise governance is the set of responsibilities and practices exercised by the board and executive management with the goals of providing strategic direction, ensuring the objectives are achieved, ascertaining that risks are managed

Manuscript received June, 1 2012.

M. Spremic is with the Department of Informatics, Faculty of Economics and Business Zagreb, University of Zagreb Kennedy's sq 6, 10000 Zagreb, CROATIA (phone: +385-1-238-3278; fax: +385-1-233-5633; e-mail: mspremic@efzg.hr).

M. Ivanov is with the Department of Finance, Faculty of Economics and Business Zagreb, University of Zagreb Kennedy's sq 6, 10000 Zagreb, CROATIA (e-mail: mivanov@efzg.hr).

B. Jakovic is with the Department of Informatics, Faculty of Economics and Business Zagreb, University of Zagreb Kennedy's sq 6, 10000 Zagreb, CROATIA (e-mail: bjakovic@efzg.hr).

appropriately and verifying that the enterprise's resources are used responsibly, IT governance is the responsibility of executives and boards of directors and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives [9]. Therefore, IT Governance covers a broad, but not always clearly defined, set of management processes that are aimed at ensuring the effective use of IS and IT within that enterprise. The primary focus of IT governance is on the responsibility of the board and executive management to control formulation and the implementation of IS strategy, to ensure the alignment of IS and business, to identify metrics for measuring business value of IS and to manage IS related risks in an effective way [16].

In this paper we stress the importance of conducting regular information system audit (IS audit) by which the level of operational risks may be assessed. Regulatory framework for conducting information system auditing in credit institutions in the Republic Croatia is explained and discussed, with a detailed analysis of its implications on a sampled credit institution.

II. 2. Managing Risks in Credit Institutions

As Laplente and Costello noticed [10] 'many financial institutions incurred large losses during the current, ongoing economic crisis with various external factors being held responsible for the losses; however, it was observed that despite this, there were a number of banks that thrived during this period and actually prevented many losses thanks to their strong risk management activities'.

Banks and other credit institutions face a number of financial and operational risks in their everyday business activities. The *credit risk* means a possibility that bank borrowers or other counterparties will fail to meet its obligations in accordance with agreed terms. It includes the potential losses arising from credit-sensitive types of bank claims such as loans and debt securities. The management of credit risk is the most complex risk management in banking industry. The goal of credit risk management is to maximize a bank's risk-adjusted rate of return by maintaining credit risk exposure within acceptable parameters, while in the same time bank have to keep stability, solvency and good performance for the future. During the history main causes of banking crisis have been too lax banks' credit standards for borrowers and counterparties, a poor portfolio risk management, or a lack of attention to changes in economic or other circumstances that can cause deterioration of bank credit portfolio.

The *market liquidity risk* is the possibility that a given securities or other forms of the bank's asset cannot be traded quickly enough in the market to prevent a loss or make the required profit. Additionally, activities of banks are by influence of the funding liquidity risk. It is driven by the possibility that over specific time horizon the bank will not be able to meet successfully expected and/or unexpected cash flows without affecting its regular daily operations or its financial performance.

Market risks include different types of risks connected with a fall in value of bank portfolio due to changes of interest rates, exchange rates or stock prices on financial markets.

The *interest rate risk* can be analyzed as a part of the market risk connected with the bank's claims on fixed rate loans or other fixed rate debt instruments which are sensitive to a price risk derived from changes in market interest rates.

A *currency risk* as the type of market risk is associated with foreign currency denominated instruments in a bank's balance sheet or in the category of different off-balance sheet items. The currency risk includes possibilities of potential gains or losses resulted from changes in the exchange rate of one currency in relation to another.

The *reputation risk* is the possibility of experiencing harms or losses due to negative public perceptions of the particular institution due to which existing and future new business relationships with clients, counterparties, shareholders and investors can be called into question.

Finally, the *operational risk* includes the risk of losses resulting from inadequate or failed internal processes including inadequate information system support for conducting business transactions. There are a lot of operational risk events which can result in a misstatement of bank's risk profile, and expose the institution to significant losses or a reputation risk. In the Sound Practices for the Management and Supervision of Operational Risk (2003), the Basel Committee on Banking Supervision has emphasized several typical examples of such events. More detailed they include:

- Internal frauds in the forms of an intentional misreporting of positions, employee theft for own account, embezzlement of money for the name of other person, hazardous trading on an employee's own account, conducting the financial transactions against the internal or external regulatory frameworks, insider trading of a corporation's stock or other securities, hiding of a bank's exposure to other risks (like liquidity risk, credit risk and market risks);
- Misuse and failures in business activities including a misuse of confidential customer information, improper trading activities on the bank's account, money laundering, financing of terrorism or other forms of crime activities, sale of unauthorized products, tax evasion, issuing and payment of demand drafts over the prescribed limits, failures to meet regulatory requirements;
- External frauds like robbery, forgery, cheque kiting, and damage from computer hacking;
- The negative selection in employment policies and failures in organization of workplace safety including the violation of employee health and safety rules, discrimination claims etc.;
- Damages to physical assets caused by terrorism, vandalism, earthquakes, fires, floods or other forms of environment risks;
- Business disruptions like system failures of hardware and software, telecommunication problems, and utility

outages;
- Troubles in execution, delivery and process management including data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty mis-performance, and vendor disputes.

For difference of credit risk and market risk that banks accept and manage to generate profit (depending on their actual level of risk appetites), a management of operational risk (and its particular forms including information system risk) has to protect banks from direct financial losses and indirect losses connected with a damage of the institution's reputation. However, an operational risk is not a standalone risk because it is derivative of all internal processes that might cause exposure of credit institutions to different financial risks and losses. An operational risk can result from inadequate allocations of assets due to an underestimation of liquidity reserves or miserable credit policies (failures of people). The operational risk includes criminal activities in credit or collateral policies, the employee's incompetence to implement techniques for measuring and managing market risk or credit risk, as well as different failures in asset and liabilities management as a whole.

Particular risks are best managed within the departments in which they arise. However, there is a significant interdependency between different risks due to which overall planning, coordination, and monitoring of whole bank's exposure to risks should be centralized in one specialized department as well as provided by an adequate internal informational system auditing. On this way operational risks can be more efficiently coordinated with financial risks.

For example large banks typically use derivatives to protect themselves from potential losses caused by negative impacts of market risks or a credit risk. Additionally, banks use derivatives also for speculative reasons as a profitable and legal kind of betting on the value of underlying assets. Due to typical bottoming on the leverage, speculation in derivatives can be very risky if allow speculators to be highly exposed to risk without adequate level of liquidity reserves. In this case the absence in possibilities of habitual borrowing on financial markets or significant unexpected changes in underlying values of derivative instruments can cause significant losses and a fall in institution's reputation (as at beginning of a financial crisis in 2007). In spite of a typical view that speculations in derivatives represent financial risks, a big part of bank's exposure can be connected with operative risk. During a history most of significant losses in speculative trading of derivatives have arisen from internal frauds or other forms of operational failures when derivatives traders circumvented risk-management controls and overdraw internal limits in the case of poor monitoring systems. Additionally, a crisis starting in 2007 emphasized the connection between operational risk management and liquidity risk management. The liquidity risk was significantly under-provisioned by banks in former years of economics expansion until 2006. Banks have made oversights in implementation of good practices for liquidity risk management reflecting also problems in management of operational risk.

Some forms of operational risks occur frequently (like settlement errors, systems failures, customer lawsuits, etc.) and they can be modeled statistically. Other forms of operational risks occur infrequently (like natural disasters, terrorism and trader frauds) what means a more difficult implementation of quantitative techniques for assessing risks. (For example, in this case large banks can use techniques based on actuarial science and engineering reliability analysis that are more typical in activities of insurance companies.) Apart from quantitative models for assessing risks, banks use the qualitative techniques for assessing risks including loss event reports, management oversight, employee questionnaires, exit interviews, management self assessment, and internal audit.

The quantitative approaches for measuring and managing operational risk was emphasized in Basel II accord on bank capital adequacy as well as in new Basel III regulatory standard on bank capital adequacy, stress testing, and market liquidity risk. The regulations have been designed to ensure that banks have adequate capital to be able to cover credit risk, market risk and operational risks that come out of its lending, investment and other business activities.

In last four years supervisors prescribe new quantitative and qualitative requirements for risk management in credit institutions where significant parts of qualitative regulation imply a request that banks have to build the adequate operational framework for the corporate governance, the establishment of an adequate and efficient internal control system, the risk reporting system, IT governance management, information system auditing, etc. Namely, in spite of a typical supervisor's orientation on quantitative measure in management of credit risk, liquidity risk and other financial risks (because quantitative data about banks' exposure to risks are more practical for external monitoring and control), qualitative requirements are very important because they emphasize the organization structure, responsibilities of management and functions of information system as preconditions for good risk management.

III. Literature Review on Information System Auditing and Assessing The Level of Operational Risks

Information system audit (IS audit) mainly refer to truly analytical part of IT Governance by which the level of IS performance can be measured and IS maturity assessed. IS audit represents a wide range of audit, managerial, analytical and technological activities with the main objective of thoroughly reviewing the effectiveness of control procedures in various parts of IS, conducting analytical tests and collecting evidences which helps in evaluating the level of operational risks and, finally, recommending company's Board's the corrective counter-measures to lower the unacceptable operational risks. There are very few evidences in literature review on investigating the role of IS auditing in managing operational risks. Caldwell [2] reports that enterprise IT security professionals face a complex, even

paradoxical situation as the worldwide economic crisis continues. In a period of highly constrained financial and staffing resources, they must manage and mitigate a rapidly changing and expanding risk environment and respond to expanding regulatory and other legally relevant requirements. Dameri [4] analysis the benefits of IS compliance preferably through IT Governance role. Mashour and Zaatreh [11] investigate and validate the positive impact effective IS may have at Jordan Banks. The institute of internal auditors (IIA) [8] issued the guidelines for assessment of IT risk (GAIT) and reported that applying a standard methodology will assist the auditor to focus on what is truly important to meeting the compliance objectives and minimizing operational risk to the organization. Gartner [5] concludes that there is no standard that covers every area of IT Governance and IS audit with many overlapping areas. Singleton [13] argues about the model of IT sophistication according to regulatory provisions and aggregates minimum IT controls composed with IT governance concept to mitigate risks in financial reporting and enhance regulatory compliance, but in [15] that concept was widened to information system auditing procedures as well. Singleton [12] also states that 'it is becoming increasingly necessary to test more IT controls due to Sarbanes-Oxley requirements, the American Institute of Certified Public Accountants (AICPA)'s Risk Suite requirements and increased reliance on IT controls. Majority of cited references take the regulatory provisions as an anchor. We tried to fill the research gap by investigating how IS auditing regulation provision may help in managing operational risk and possibly question its usage and effectiveness.

In following chapters an IS auditing regulatory framework will be explained and analyzed, especially national regulations in the Republic of Croatia. We will investigate if national regulatory provisions in IS auditing help improving IT Governance and operational risk management procedures.

IV. Regulatory Frameworks in IT Governance and IS Auditing Domain

Main objective of IS auditing activities is to review the company's control procedures associated to IS, collect analytical evidences about possible misuse, evaluate the level of operational risks for different control areas and suggest to company executives corrective control counter-measures [15].

This in particular mean that by engaging in IS auditing companies can periodically measure the IT Governance performance and IS maturity using the world-wide and/or national regulatory framework and well-proved, world-wide frameworks or methods such as CobiT, Risk IT, ITIL, ISO 27001, etc. Such tendencies are mostly motivated by specific regulatory pressures (for example, Sarbanes-Oxley act, Basel II framework, etc.), rather than by IT value-added initiatives.

IT Governance and IS auditing are partly driven by the external regulatory demands like Sarbanes-Oxley act, Basel II, the European 8th Directive and MiFID. Companies operating on multinational markets have to comply with several legal regulations created by public laws on national or international level. For instance, the Sarbanes-Oxley Act (SOX) in the USA and Basel II (the current version is "Basel III") in Europe. "New Capital Accord", also known as Basel II, is a set of recommendations issued by "The Basel Committee on Banking Supervision" regulating the adequacy of banks' capital in relation to risk exposure. Basel II provisions apply to internationally active banks in G10 countries. The European Union adopted a Directive (CAD3) rendering the provisions of the Accord compulsory for all banks in EU member countries by 2007. The Accord deals with requirements for the bank's information system as a part of the operational risk as a whole only through IT Governance principles considering that it is not possible to set strict rules on account of rapid technological changes and differences between banks. The Committee emphasizes the importance of reliability of the IS, particularly in terms of information security and system availability. This means that the stipulations of the Accord have provided banks with great freedom in deciding on the measures for reducing operational risk posed by implementation of IS/IT, but on the same time dictated banks that certain IT Governance activities should be put in practice in order to be compliant.

In recent years various groups have developed world-wide known IT Governance best practices and frameworks to assist management in managing operational risks and measuring the maturity of IS. Contemporary IT Governance frameworks are:

- CobiT (Control Objectives for Information and related Technology),
- ISO 27000 'family' (ISO 27001:2005, ISO 27002:2005),
- ITIL (IT Infrastructure Library), or
- PCI DSS and IT BSC (IT Balanced Scorecard)

A. Cobit methodology for conducting IS audits

CobiT (Control Objectives for Information and related Technology) is the widely accepted IT Governance framework organized by key IT control objectives, which are broken into detailed IT controls. Version 4.1 of CobiT divides IT into four domains (Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate), which are broken into 34 key IT processes, and then further divided into more than 300 detailed IT control objectives, with a new CobiT 5.0 underway acting as a comprehensive IT governance methodology. ISACA and ITGI [9] defines COBIT as a comprehensive set of resources that contains all the information organizations need to adopt an IT governance and control framework.

Developed by ISACA (Information System Audit and Control Association, www.isaca.org) and ITGI (IT Governance Institute, www.itgi.org), CobiT is the widely accepted IT governance and IS auditing framework and represents an 'umbrella' framework for implementing IT Governance policies and procedures and for conducting IS auditing. It is a broad and comprehensive de-facto standard which comprises all activities, processes and services which can help companies manage the level of operational (IS/IT related) risks.

V. National Regulations on IT Governance and IS Auditing in the Republic of Croatia

As explained in [15], in the Republic of Croatia the regulatory framework for IS auditing was prescribed by Croatian National Bank (CNB). The main objective of the obligatory regulations is to effectively manage the level of operational risks, namely IS/IT associated risk in credit institutions (banks, etc.). The 'Act about credit institutions' and the 'Decision on adequate information system management' are the cornerstones of the IT Governance regulation that obliged every credit institution to perform internal and especially external IS auditing (assessment of operational risks) and to prepare a report for the regulator as well as for company's Board. The regulation itself is CobiT based and concerned to a framework and scope of evaluating the maturity of using IS/IT, which in fact means testing IT controls in order to be able to assess the level of specific IT risks.

Regulatory framework prescribed the 18 areas and 40 articles in total which define the scope of every information system audit in the credit institutions in Croatia. These areas are as follows:

1. Managing information system security
2. Managing the risks associated to information systems
3. Managing logical and physical access rights
4. Managing the information systems assets
5. Managing operating and system records
6. Managing back-up and archive
7. Managing the relationships to service providers and outsourcers
8. Managing the relationships to hardware vendors
9. Managing the information system development
10. Managing physical security
11. Managing passwords
12. Configurations management
13. Change management
14. Business Continuity planning
15. Disaster Recovery plan
16. Managing incidents and problems
17. Antivirus policy
18. Documentation and internal acts associated to information systems

According to the regulatory framework, the Board of every credit institution in Croatia is responsible for mitigating operational risks associated to every single area and to effectively manage the level of the acceptable IS/IT risk. Some detailed and precise regulatory responsibilities include [15]:

- to nominate the member of the Board who is responsible for managing and controlling IS,
- to adopt internal regulations governing the IS management, and define responsibilities for supervising the implementation of these regulations,
- to define the criteria, methods and procedures for notifying the management and supervisory boards of the relevant facts related to the functionality and security of the information system,
- to define IS strategy,
- to define clear and precise responsibilities for managing IS,
- to nominate the autonomous CISO function (Chief Information Security Officer),
- to nominate the IT Steering Committee,
- to define the IS risk management methodology and processes,
- to nominate IT Governance Committee
- to assess IS risks and to reduce them to acceptable level,
- management board shall be responsible for establishing the acceptable level of risk to which the information system is exposed (operational risk),
- to classify and protect information,
- internal audit is responsible to conduct IS audits,
- to establish the system of user access rights management, comprising the registration, authorisation, identification, authentication and supervision of user access rights,
- a process of managing the changes in the IS's software components need to be set up (initial versions should be determined, any changes in application software and database environment should be identified and monitored, etc.)
- changes in the IS's software components need to be recorded and documented in order of occurrence, together with the time of their occurrence,
- Board is responsible to establish the process of business continuity planning (BCP) and management,
- Board is responsible to create the business impact analysis, to accept the business continuity plan, to accept the disaster recovery plan and to test their functionality and effectiveness,
- Board is responsible for establishing appropriate incident management process to ensure a timely and effective response in the event of the violation of security and functionality of the IS resources supporting the carrying out of the business processes,
- Board is responsible for establishing the process of data recovery which will be stored on the alternative location.

A. Methodology for Conducting IS Auditing

In Republic of Croatia every single credit institution is obliged to conduct external and internal IS audits with the objective of measuring the level of operational risks. Internal and external IS auditing are conducted according to framework explained in previous chapter. Every single external IS audit should result in comprehensive report which IS auditors are to present to credit institution's Board. Main areas of external IS audit reports are:

- explanation of IS audit methodology and methods for measuring the level of operational risks,
- scope of IS audits – choosing the areas for extensive IS auditing (depending on IS audit assignment). In the case of conducting IS auditing of credit institutions in

the Republic of Croatia, the audits scope is fully prescribed by regulatory framework (11 areas mentioned in chapter 4.). Upon the preliminary risk assessment, IS auditor has the autonomy to choose which area needs extensive testing and further review of control procedures. In other cases, IS audit scope needs to be agreed with the provisions of assignment itself (for example, by Board's request, etc),
- results of detailed and thorough review of control procedures in chosen audit areas,
- assessment of the level of operational risk for every audit area, with the recommendations to the Board for corrective measures,
- Board's response to IS audits findings,
- summary and review of IS audit documentation.

IS auditors needs to get full and in-depth understanding of control procedures in key business processes and there IS/IT support. As stressed in previous chapters, main objective of IS auditing is to thoroughly review the effectiveness of control procedures in various parts of IS in credit institutions, to measure the level of operational risks and to recommend the corrective measures to Board members. This in particular means that IS auditors need to examine and review the large number of controls inside IS, conduct massive analytical tests (for example, penetration test of computer network, business continuity and disaster recovery tests, test of IS users logical access rights, etc.), collect a number of audit evidences, assess the level of operational risk and prepare the comprehensive IS audit report.

Every single audit area should be thoroughly reviewed with the objective of gathering enough audit evidences which will enable IS auditors to evaluate the efficiency of control procedures. For example, typical key business processes in credit institutions whose IS support needs to be evaluated are:
- Corporate and retail deposits,
- Corporate and retail loans,
- Treasury process,
- Risk management process,
- Payment processing,
- Financial statement close process.

IS audit findings, risk assessments and recommendations are independent, objective and based on professional and expert evaluation, but on the same time without any personal interest on any kind. Findings and professional risk assessments are based on following activities:
- pre-audit questionnaire filled by responsible employees (CIO – Chief Information Officer),
- review of documentation provided by credit institution,
- selection of appropriate control objectives and strategies and methods of testing control efficiencies,
- interviews with adequate users and employees,
- review of system settings and parameters (full list of electronic and paper-based evidences needs to be provided at the end of report),
- physical review of key IT equipment,
- monitoring IS activities and performing tests of controls,
- technology-based testing of control efficiencies (for example, computer network penetration testing, firewall secure protocols testing, data exchange testing, etc.).

The maturity level of IS management procedures in all 11 audit areas are regularly based on interviews, testing procedures and comprehensive reviews. Maturity levels for all audit areas can be based on CobiT metrics:

0 – Non-existent IS maturity and/or IS control procedures,
1 – Ad hoc / initial IS maturity and/or IS control procedures,
2 – Repeatable but intuitive IS control procedures,
3 – Defined process for IS control procedures,
4 – Managed and measureable IS control procedures,
5 – Optimised IS maturity and/or IS control procedures.

The IS audit report need to be presented to and agreed with the credit institution's Board, while the copy of the report needs to be forwarded to regulatory body (Croatian National Bank and their supervisory units).

B. The Results of Continuous Quality Control Processes over IS Auditing Reports

Croatian National Bank monitors the whole process and fosters credit institutions to implement IS auditors' recommendation and secure the quality of IS audits. By CNB regulations external IS auditors have to evaluate the maturity of IT Governance practices with following qualitative marks:
- completely unsatisfactory,
- partially unsatisfactory,
- partially satisfactory,
- satisfactory and
- completely satisfactory.

External IS auditors have to present their comprehensive report to bank's Board and CNB authorities. CNB performs quality assurance on these reports and may refuse it and penalize authors while bank's Board have to make formal response to the IS auditors findings. CNB monitors the IS audits and fosters credit institutions to implement IS auditors' recommendation.

The assessed level of operational risks in credit institutions in the Republic of Croatia which arises from external IS auditing activities in 2010 were as follows:
- 11 credit institutions satisfactory manage the level of operational risk,
- 18 credit institutions partially satisfactory manage the level of operational risk and
- 2 credit institutions partially unsatisfactory manage the level of operational risk.

Upon the results of external IS audits and according to their internal plan, CNB supervisory unit conduct 'on-site' IS supervisions in which they thoroughly audits the IS of specific credit institutions and give recommendations which credit institutions are obliged to conduct, or they will be fined. By doing so, credit institutions, especially their CIOs and Board members are deeply engaged in IS Management and IT Governance issues.

On the other hand, if they do not meet prescribed quality

standards, CNB can refuse external IS audit report and mandate the credit institution to, on its additional expense, hire another company to do repeated external IS audit, which is a good mechanisms for regulating and monitoring the IS auditing services and foster quality standards.

VI. Conclusion

Main objective of this paper was to stress the importance of prescribing IS auditing regulatory framework which helps credit institutions manage the level of operational risk. After analyzing IT Governance and IS auditing terms, we explained external and especially national regulation framework in the Republic of Croatia and present the methodology of conducting IS auditing.

As mentioned in chapter 5. Croatian National Bank (CNB) prescribed IS auditing regulatory framework ('Decision on adequate information system management') upon which regular external and internal IS audits are obligatory for every single credit institution operating in the Republic of Croatia. By this regulation the IT Governance performance (maturity) levels are prescribed (completely unsatisfactory, partially unsatisfactory, partially satisfactory, satisfactory and completely satisfactory). The main objective of such a strong regulation is to strengthen the maturity of IT Governance and IS auditing processes in credit institutions. Some results of such approach may be the fact that all credit institutions in Croatia has IS strategy or have a CISO (Chief Information Security Officer) as an autonomous person nominated for managing IS security. All of them are conducting regular IS audits and every single credit institution operating in Croatia has to have Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) integrated into operational risk management process and IT Governance policies.

Very strict and rigorous IT Governance regulations in Croatia enforce that IS management is on very mature level in almost all commercial banks operating in the country. Consequently, BCP practices are on very high level, meaning that every single commercial bank operating in Croatia has a BC strategy, BC plan and DR plan. Majority of them identified key IT control metrics for BCM (RTO, RPO) according to the business impact analysis. Also, majority of commercial banks operating in Croatia has a DR site and modern data replication systems. This is particularly interesting having in mind their ownership structure. Largest banks operating in Croatia are owned by banks with head offices in nearby countries (Italy, Austria, France, and Germany), while in the same time, very strict regulations are meant that IT Governance practices in their Croatian subsidiaries are much stronger than in parent companies.

In 2010 there were only two credit institutions with partially unsatisfactory mechanisms for managing operational risks. The assessed level of operational risks is associated with the partially unsatisfactory maturity of IS control procedures, which arises from thorough and serious IS audits according to regulatory provisions and world-wide best accepted methodologies (such as CobiT).

We investigate in further details the IT Governance practice in one of the two credit institutions which are partially unsatisfactory managing operational risk. In this small bank CIO (Chief Information Officer) reports directly to member of the Board responsible for IS, they have proper IS strategy, autonomous CISO (Chief Information Security Officer) function who reports directly to Supervisory Board, there are a number of cross-functional organizational units who helps to manage IS function (such as IT Steering Committee, IT Project Management Committee, Business Continuity Board, IT Change Management Committee). In recent year bank prescribe BCP (Business Continuity Plan) and conduct massive efforts to properly control IS function and associated operational risks.

As mentioned in previous chapters, the main objective of conducting external IS auditing is to assess the level of operational risks, or, in other words, to assess the level of IS Maturity. One can do so by using world-wide accepted standard methodology such as CobiT. CobiT based IS maturity marks for selected small bank (scale from 0 to 5) were as follows:

- In a year 2008. - 1.9;
- In a year 2009. - 2.1;
- In a year 2010. - 2.2.

Even the improvement in IS Maturity and IT Governance activities are evident (CobiT is very rigorous methodology), partially unsatisfactory level of managing operational risk stands due to the fact that there still are insufficient control procedures in some key areas of IT Governance (such as BCP, information security, computer network access, IS/IT outsourcing, etc.). On the hand, the bank's management has the clear vision and enough funds to fulfill IS auditor's recommendations and hope for satisfactory level of managing operational risks in 2011.

After explaining the IS auditing regulatory framework in the Republic of Croatia, by presenting the practice of monitoring the quality of IS audits and by conducting long-lasting (3 year) dedicated in-depth interviews in a small bank, we come up to a conclusion that national IS Auditing regulatory framework can help in improving operational risk management practice. The research might be useful because of fact that similar efforts are very rare (if there are any of them) and there are modest evidences how industry best practices and national regulations are used in the real business environment.

References

[1] C. Amancei, and T. Surcel, Key Components and Operability Evaluation of Internal Controls for Risk Assessment Modeling in IT Audit, *WSEAS Transaction on Business and Economics*, Issue 4, Vol. 7, pp 349-358, October 2010.

[2] F. Caldwell, "Selecting and Applying GRC Frameworks and Standards," *Gartner Symposium ITExpo*, Orlando, October 2009.

[3] J.J. Champlain, *Auditing Information Systems*, 2nd ed. John Wiley & Sons, SAD, 2003.

[4] Dameri, R.P., (2009): Improving the Benefits of IT Compliance Using Enterprise Management Information Systems, The Electronic Journal Information Systems Evaluation, Volume 12, Issue 1, 2009, pp. 27-38.

[5] Gartner (2010): Magic Quadrant for Continuous Controls Monitoring, March 2010, Gartner Inc.

[6] Guldentrops, E. (2004): "The IT Dimension of Basel II," *Information System Control Journal*, vol. 6, 2004.
[7] J.E. Hunton, S.M. Bryant, and N.A. Bagranoff, *Core Concepts of Information Technology Auditing*, John Wiley &Sons Inc., SAD., 2004.
[8] Institute of Internal Auditors IIA, *Case Studies of using GAIT for business and IT Risk to scope PCI compliance*, IIA Advanced Technology Committee, 2008.
[9] ITGI, *CobiT 4.1. Framework, Control Objectives and Maturity Models*, IT Governance Institute, Rolling Meadows, Illinois, SAD, 2007.
[10] P.A. Laplante, and T. Costello; *CIO Wisdom II: More Best Practices*, Prentice Hall, USA, 2005
[11] Mashour, A., Zaatreh, Z. (2008): A Framework for Evaluating Effectiveness of Information systems at Jordan Banks: An Empirical Study, Jorunal of Internet Banking & Commerce, April 2008, Vol 13, Num. 1.
[12] M. Nicho, and B. Cusack, "A Metrics Generation Model for Measuring the Control Objectives of Information Systems Audit," *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, Hawaii, IEEE, January, 2007.
[13] T. Singleton, "What every IT Auditor Should Know About Access Controls," *Information System Control Journal*, vol. 4, ISACA, 2008.
[14] T. Singleton, "The Minimum IT Controls to Assess in a Financial Audit," *ISACA Journal*, vol. 2, ISACA, 2010.
[15] M. Spremić, Measuring IT Governance Performance: a Research Study on CobiT- Based Regulation Framework Usage, *International Journal of Mathematics and Computers in Simulation,* Issue 1, Volume 6, 2012, pp 17-25.
[16] M. Spremić, "IT Governance Mechanisms in Managing IT Business Value," *WSEAS Transactions on Information Science and Applications*, Issue 6, vol. 6, pp. 906-915, June 2009.
[17] M. Spremić, and M. Popović, "Emerging issues in IT Governance: implementing the corporate IT risks management model," *WSEAS Transaction on Systems*, Issue 3, vol. 7, pp. 219-228, March 2008.
[18] P. Weill, and J. W. Ross, *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, 2004.